Interworking of Wireless and Mobile Networks based on Location Information
To Moni, Lilli, 
and my entire family
The rapid development of mobile radio within the last ten years is indicative of the imminent paradigm shift towards an information society. While first- and second-generation mobile radio systems mainly focused on speech services, third-generation systems were inherently designed to supply multi-media data services to the mobile customer. The key challenge in this is Quality of Service (QoS) provisioning including service guarantees within well-defined limits. In mobile service provisioning, particular problems derive from the limited maximum supplied data rates.

The ubiquitous access to mobile services and the support of very high data rates (Mbit/s → Gbit/s) are two opposing challenges within wireless communications. Integration of heterogeneous access techniques promises to be a possible remedy. Short distance coverage at high bit rate within Hot Spots is typically provided by Wireless Local Area Networks (WLAN). These are complemented by Fixed Wireless Access (FWA) technologies realizing wireless local loop solutions for the last mile. However, area-wide coverage based on WLAN or FWA technology is unlikely for economic reasons. Accordingly, one can expect that fourth generation mobile communication will be characterized by the symbiosis of different heterogeneous radio systems.

This thesis contributes to this development by presenting a new concept to support system integration and cooperation. Exemplary evaluations take place using UMTS and IEEE 802.11. Its outcome is a sophisticated control scheme that implements cross-system decision-taking functions, e.g. for vertical handover control. The key idea is to concatenate measurement reports as inherently available within each radio system with location information. The resulting link state maps can be used by complementary radio systems making self-conducted mutual scanning obsolete. Another advantage is given if these link state maps are applied for further tasks such as optimization of existing networks or planning of new deployments.

Within the thesis, the related concept is elaborated from an abstract idea to specific use cases. Analytical investigations, supplemented by a prototypical im-
plementation with event driven simulations, demonstrate the mutually resulting benefit for associated systems. It is shown that the cooperation of radio access networks using third party measurements and location data is a case of a win-win situation. Furthermore, it is noteworthy that the application of ideas presented in this work unlocks the potential for new use cases that cannot be otherwise realized.


Die vorliegende Arbeit unterstützt diese Entwicklung mit der Einführung und Bewertung eines neuartigen Konzeptes zur Integration unterschiedlicher Technologien, exemplarisch für UMTS und IEEE 802.11. Hierbei entstand ein intelligentes Steuerkonzept, welches z.B. bei der Entscheidungsfindung für vertikale Handover optimale Anwendung findet. Die Grundidee dabei ist es, Messberichte, wie sie in jedem Funksystem zur Verfügung stehen, mit Ortinformationen zu koppeln und heterogenen Komplementärsystemen verfügbar zu machen. Einer von vielen Vorteilen, der sich daraus ergibt, ist, dass auf eigenständiges Scannen anderer Funktechnologien weitestgehend verzichtet werden kann. Darüber hinaus beinhaltet die Erfassung ortsspezifischer Funkfeldeigenschaften ein beträcht-
liches Potential der Weiterverwertung, etwa für die Optimierung bestehender Netze oder die Planung neuer Standorte.

# Table of Contents

1. **Introduction** ........................................................................ 1  
   1.1 Motivation .............................................................................................1  
   1.2 Objectives ..............................................................................................2  
   1.3 Contribution of this Thesis .................................................................3  
   1.4 Outline .................................................................................................3  

2. **System Overview**................................................................ 7  
   2.1 UMTS ....................................................................................................7  
      2.1.1 General Overview ........................................................................10  
      2.1.2 Synchronization & Cell Search ....................................................13  
      2.1.3 Scanning of Complementary Systems & Compressed Mode ......19  
      2.1.4 Measurements in UMTS ..............................................................23  
      2.1.5 Measurement Reports .................................................................28  
   2.2 IEEE 802.11 ........................................................................................30  
      2.2.1 General Overview ........................................................................30  
      2.2.2 Synchronization & Cell Search ....................................................37  
      2.2.3 Scanning Procedures in WLAN 802.11 .......................................39  
      2.2.4 Measurements in 802.11 ..............................................................44  
      2.2.5 Specific Measurements in 802.11h ..............................................50  

3. **Integration & Cooperation of Radio Access Networks** . 57  
   3.1 Introduction .........................................................................................57  
   3.2 State of the Art Overview.................................................................59  
      3.2.1 Standardization Bodies & Fora ....................................................59  
      3.2.2 Research Projects .........................................................................66  
      3.2.3 Comparison of Integration Efforts ..............................................72  
   3.3 Mobility & Handover ........................................................................76  
      3.3.1 General Aspects of Mobility .........................................................78  
      3.3.2 Handover Aspects .........................................................................81  
   3.4 Trigger .................................................................................................94
4. Localization Techniques & Principles ...................... 101

4.1 Localization & Positioning ...................................................... 102
  4.1.1 Localization – What for? ...................................................... 102
  4.1.2 Location Based Services ...................................................... 103

4.2 Basic Localization Principles ..................................................... 110
  4.2.1 Classification of Localization Techniques ......................... 112
  4.2.2 Physical & Symbolic Localization ........................................ 114
  4.2.3 Absolute & Relative Localization ........................................ 115
  4.2.4 Self- & Remote Localization ................................................ 115

4.3 Cellular Localization ................................................................. 116
  4.3.1 Cell Id ......................................................................................... 116
  4.3.2 Signal Strength ........................................................................... 118
  4.3.3 Time-based Algorithms ............................................................. 119
  4.3.4 Angle of Arrival ......................................................................... 124
  4.3.5 Database Correlation/ Fingerprints/ Pattern Recognition ............. 124
  4.3.6 Hybrid Methods ......................................................................... 125

4.4 Satellite Localization ................................................................. 126
  4.4.1 Global Positioning System ......................................................... 127
  4.4.2 GLONASS .................................................................................. 133
  4.4.3 Galileo ......................................................................................... 133

4.5 Accuracy & Precision ............................................................... 134

4.6 Summary .................................................................................. 137

5. Hybrid Information System ..................................................... 139

5.1 Motivation .................................................................................. 140
5.2 Basic Principle ........................................................................... 140

5.3 Overview ................................................................................... 141
  5.3.1 Feeding & Information Clients .................................................. 141
  5.3.2 Localization Units ....................................................................... 142
  5.3.3 Service Control & Data Administration Units ......................... 143
  5.3.4 Passive & active operation .......................................................... 145

5.4 Data Administration ..................................................................... 146
  5.4.1 Feeding of the Hybrid Information System .............................. 146
  5.4.2 Internal Data Processing ............................................................ 146
  5.4.3 Data Supply ................................................................................ 150
  5.4.4 Self-Healing property ................................................................. 150

5.5 Application Areas ...................................................................... 151
  5.5.1 Handover triggering ................................................................. 151
  5.5.2 Network/Coverage optimization ............................................. 151
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5.3</td>
<td>Link Adaptation &amp; Power Control</td>
<td>152</td>
</tr>
<tr>
<td>5.5.4</td>
<td>Adaptive Beaconing</td>
<td>152</td>
</tr>
<tr>
<td>5.6</td>
<td>Realization Aspects: Mapping to 3/4G Architectures</td>
<td>153</td>
</tr>
<tr>
<td>5.6.1</td>
<td>Location Services Architecture of 3GPP</td>
<td>153</td>
</tr>
<tr>
<td>5.6.2</td>
<td>WLAN/3GPP Interworking Architecture</td>
<td>163</td>
</tr>
<tr>
<td>5.6.3</td>
<td>WINNER Logical Node Architecture</td>
<td>165</td>
</tr>
<tr>
<td>5.6.4</td>
<td>Summary</td>
<td>168</td>
</tr>
<tr>
<td>6.</td>
<td>Performance Analysis</td>
<td>171</td>
</tr>
<tr>
<td>6.1</td>
<td>Localization Aspects</td>
<td>172</td>
</tr>
<tr>
<td>6.1.1</td>
<td>Modeling of Localization Imprecision</td>
<td>172</td>
</tr>
<tr>
<td>6.1.2</td>
<td>Evaluation Criterion</td>
<td>174</td>
</tr>
<tr>
<td>6.2</td>
<td>Correlation Analysis</td>
<td>176</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Normal Distribution with cut-off</td>
<td>178</td>
</tr>
<tr>
<td>6.3</td>
<td>Virtual Coverage</td>
<td>182</td>
</tr>
<tr>
<td>6.4</td>
<td>Beacon Protection</td>
<td>185</td>
</tr>
<tr>
<td>7.</td>
<td>Integrated Simulation Environment</td>
<td>191</td>
</tr>
<tr>
<td>7.1</td>
<td>Overview</td>
<td>191</td>
</tr>
<tr>
<td>7.2</td>
<td>S-WARP</td>
<td>193</td>
</tr>
<tr>
<td>7.2.1</td>
<td>General Overview</td>
<td>194</td>
</tr>
<tr>
<td>7.2.2</td>
<td>Specific Changes</td>
<td>194</td>
</tr>
<tr>
<td>7.3</td>
<td>URIS</td>
<td>196</td>
</tr>
<tr>
<td>7.3.1</td>
<td>General Overview</td>
<td>197</td>
</tr>
<tr>
<td>7.3.2</td>
<td>URIS Modifications</td>
<td>198</td>
</tr>
<tr>
<td>7.4</td>
<td>S-GOOSE/RISE</td>
<td>199</td>
</tr>
<tr>
<td>7.5</td>
<td>Extended HIS</td>
<td>200</td>
</tr>
<tr>
<td>7.5.1</td>
<td>HIS</td>
<td>201</td>
</tr>
<tr>
<td>7.5.2</td>
<td>HO Manager</td>
<td>202</td>
</tr>
<tr>
<td>7.6</td>
<td>Simulator Integration &amp; Modeling</td>
<td>207</td>
</tr>
<tr>
<td>7.6.1</td>
<td>Module Loader</td>
<td>207</td>
</tr>
<tr>
<td>7.6.2</td>
<td>Combined Statistical Evaluation</td>
<td>208</td>
</tr>
<tr>
<td>7.7</td>
<td>Simulator Validation</td>
<td>209</td>
</tr>
<tr>
<td>7.7.1</td>
<td>Queue Transfer</td>
<td>209</td>
</tr>
<tr>
<td>7.7.2</td>
<td>RPI Measurements</td>
<td>215</td>
</tr>
<tr>
<td>8.</td>
<td>Performance Evaluation</td>
<td>221</td>
</tr>
<tr>
<td>8.1</td>
<td>Services &amp; Scenarios</td>
<td>222</td>
</tr>
<tr>
<td>8.2</td>
<td>Detrimental Scanning Impact</td>
<td>223</td>
</tr>
<tr>
<td>8.2.1</td>
<td>WLAN: System Detection</td>
<td>224</td>
</tr>
</tbody>
</table>
8.2.2 UMTS: Impact of Compressed Mode ........................................... 227
8.3 Enhanced Coverage Detection .......................................................... 236
  8.3.1 Coverage Detection .................................................................... 236
  8.3.2 CoG Trigger Performance .......................................................... 247
8.4 Context Provisioning ......................................................................... 252
  8.4.1 Recommendation of initial PHY-Mode ...................................... 252
  8.4.2 Capacity Exploitation ................................................................. 258
8.5 Adaptive Beacon Control .................................................................. 262
  8.5.1 Control of Beacon Interval ......................................................... 262
  8.5.2 Directed Beaconing .................................................................... 272

9. Summary & Outlook ........................................................................... 281

A. HIS: Further Application Areas and Related Work ........... 285
  A.1 Measuring of non-accessible areas .................................................... 285
  A.2 ABC Support ..................................................................................... 286
  A.3 Radio Resource Management & Connection Admission Control .... 286
  A.4 Positioning Support ........................................................................... 287
  A.5 Location Aware Networking ............................................................. 288
  A.6 Navigation Support ............................................................................ 289
  A.7 Related Work ..................................................................................... 289

B. Geodetic Fundamentals ...................................................................... 293
  B.1 Introduction ....................................................................................... 293
  B.2 World Geodetic System 1984 ............................................................ 297
  B.3 Universal Transverse Mercator ......................................................... 298
  B.4 Gauss-Krueger Coordinate System ................................................... 300

C. Specific Measurements in 802.11k ............................................. 303
  C.1 Channel Load Report ......................................................................... 307
  C.2 Noise Histogram Report ..................................................................... 308
  C.3 Beacon Report .................................................................................. 308
  C.4 Frame Report ................................................................................... 310
  C.5 Hidden Station Report ........................................................................ 311
  C.6 Medium Sensing Time Histogram Report ......................................... 312
  C.7 STA Statistics Report ......................................................................... 314
  C.8 LCI Report ......................................................................................... 316
  C.9 Measurement Pause Request ............................................................ 317

List of Figures ......................................................................................... 319
List of Tables ........................................................................................................ 323
Bibliography ......................................................................................................... 325
Abbreviations ...................................................................................................... 343
Index .................................................................................................................... 347
Acknowledgement................................................................................................ 355
Biography ............................................................................................................. 357
CHAPTER 1

Introduction

Content

1.1 Motivation ................................................................. 1
1.2 Objectives .............................................................. 2
1.3 Contribution of this Thesis ........................................ 3
1.4 Outline ................................................................. 3

“People tend to overestimate what can be done in one year and to underestimate what can be done in five or ten years”

1.1 Motivation

Mobile radio systems address two basic human needs: Communication and Mobility.
While first generation (1G) mobile radio systems suffered from a multiplicity of problems, the commercial launch of the second generation (2G) Global System for Mobile Communications (GSM) in the early nineties started what has become an unprecedented success story. The focus was initially put on voice services; however, associated services like the Short Message Service (SMS) turned out to become real ‘killer’ applications. Driven by the ambition to offer further sophisticated wireless services, 2.5G systems were conceived, operating on top of GSM. Soon it became clear that second generation systems would not offer a long-term perspective to the customers: The rapid development of the information society expressed in the Internet boom resulted in wireline services to the customers that were also supposed to be offered wirelessly.

With the design of the Universal Mobile Telecommunications System (UMTS) in the late nineties, a new 3G standard was approved that aimed at wireless provi-
sioning of services with *Quality of Service* (QoS) as known from wired connections. However, the roll out of UMTS turned out to be more of a challenge than expected resulting in a more and more delayed commercial launch. Meanwhile, wireline last mile access techniques such as *Digital Subscriber Line* (DSL) appeared, offering broadband connections to the customer at home. Having become accustomed to large bandwidths, it is almost certain that end-users will begin to request for similar broadband mobile services – a demand that cannot be satisfied by sole UMTS deployments.

Accordingly, ongoing research is being directed towards 4G systems. Since opinions differ, considering 4G either as a new air interface specification or as an enhancement to existing deployments, the term *Beyond 3G* (B3G) is often used. A key role in the development towards 4G will be taken over by wireless systems supporting high bit rates in local areas. *Wireless Local Area Networks* (WLAN) and *Fixed Wireless Access* (FWA) systems have received particular interest in recent years.

Whatever the manifestations of B3G will be, they will have to feature a high degree of interoperability: System cooperation, information exchange, and seamless service continuity across heterogeneous systems are the key challenges in this development.

### 1.2 Objectives

This thesis addresses aspects of system integration and interoperability. Rather than being reliant on one single wireless communication technology, cooperation of complementary radio access networks, each optimized for specific requirements, will play a key role. Investigations are carried out using two exemplary systems: UMTS representing a cellular mobile radio system and IEEE 802.11 representing a wireless local area network to cover hot spot scenarios. The overall goal is the complementary use of different systems to achieve the *Always Best Connected* (ABC) principle. For this, context information mainly in terms of location data and measurement reports are favorably processed. Particular importance is attached to the exploitation of legacy input data as provided by the considered systems. This ensures that new concepts derived in this thesis can be implemented without significant changes of existing specifications. Though the earlier mentioned statement by J. Licklider dates from 1965, it is still valid today. In particular the information society, with wireless communication
as one driving element, is subject to rapid and sometimes only hard to predict developments. While there is no clear 4G killer application predicted yet, decisions with respect to future development still have to be taken. A framework for cooperation of heterogeneous systems, as addressed in this thesis, will help to establish sustainability and smooth migration.

1.3 Contribution of this Thesis

This thesis introduces and elaborates on a novel framework for inter-system collaboration of heterogeneous mobile radio networks. Overarching system control with focus on vertical handover is supported by being based on joint evaluation of context information such as measurement reports and location information. Optimal network selection is achieved because related decisions rely on cross-system information concerning general existence, current availability and offered Quality of Service (QoS) support of any complementary network. Since evaluated context information is derived from legacy operation of each single system, no further overhead at the air interface is given. Furthermore, the detrimental impact due to state-of-the-art information gathering by means of self-conducted scanning can be avoided.

Manifestation of the proposed concept is given in terms of the Hybrid Information System (HIS). By providing a platform for overarching system control and inter-system information exchange HIS turns out to serve as an enabling concept for provisioning of new services in the context of next generation networks. Within this work, the concept has been developed from an initial idea to a concrete cooperation scheme. Leading IST-projects such as WINNER have taken up the HIS idea, making it a promising concept for future networking.

A prototypical HIS implementation was established in the scope of producing this thesis. The validation of the simulation environment ensures the integrity of the resultant outcomes. Both analysis and simulation were applied to demonstrate the potential of cooperating system control.

1.4 Outline

The outline of this thesis is as follows:
Chapter 2 provides an overview of the cellular Universal Mobile Telecommunications System (UMTS) and the wireless local area network according to IEEE
802.11. Particular focus hereby is put on synchronization procedures, scanning, and acquisition of measurements.

Chapter 3 describes the integration and cooperation of radio access networks. Starting with a state-of-the-art overview, related work within standardization bodies, fora, and international research projects is reflected. This is followed by a description of the general aspects of mobility and handover. For the latter, so called ‘triggers’ play an important role. Another topic to be addressed is *Vertical Handover* (VHO), which is seen as one enabling scheme for the interaction of heterogeneous systems.

Chapter 4 addresses localization techniques and principles. In addition to a general introduction on positioning methods and applied techniques, potential metrics to classify localization systems are given. According to the context of this thesis, the derivation of location information by means of mobile radio systems is one focus. Particular attention is paid to the definitions of accuracy and precision. These terms represent abstract properties of concrete positioning techniques and serve as input parameters for analysis and simulation. A summary of different (hybrid) positioning techniques with related properties is presented at the end of this chapter.

Chapter 5 introduces the *Hybrid Information System* (HIS) as one cornerstone of this thesis. The basic principle describes how HIS associates foreign party based measurements with location information in order to support system control and handover management. Respective data is administered in dedicated databases. In addition to the underlying concept, application areas for HIS are discussed followed by aspects of its realization. In detail, HIS integration in the reference architectures of 3GPP Location Services, WLAN/3GPP Interworking and the WINNER Logical Node Architecture are presented. An overview of other related work concludes this chapter.

Chapter 6 provides different analytical investigations. The addressed topics include imprecise positioning, service maintenance in case of non area-wide Hot Spot coverage, and harmful impacts of beacon broadcasts. Considering location aspects, the reliability of location data based decision making is discussed. The investigations on service maintenance serve as basis for future WLAN deployments on the one hand, and worthwhile VHO triggering for existing deploy-
ments on the other. For the beaconing, it is demonstrated that wasted capacity results, a drawback that can be counterbalanced by the application of HIS.

Chapter 7 entails a description of the integrated simulation environment. The different simulators for UMTS, IEEE 802.11 and the channel model are briefly described along with modifications undertaken. Special emphasis was put on the description of the HIS and its functional entities, all of which have been implemented in the scope of this thesis. Finally, validation of the integrated overall simulation environment is performed to ensure reliable and therefore trustworthy results.

Chapter 8 provides simulation results revealing benefits of system control with the Hybrid Information System. First, some general assumptions on simulation scenarios and parameters are presented. Hereafter, drawbacks of conventional system control approaches based on self-conducted scanning are disclosed. These drawbacks are avoided in case of HIS based system control. Furthermore, a new mechanism for coverage detection is introduced that allows HIS to fire handover triggers in the most optimized way. Additional benefit generates from context information to be provided by HIS together with triggers. Finally, another example for HIS based system control is presented within which beaconing is beneficially adjusted. Particular value is given to the joint application of directed antennas resulting in uses that would be unfeasible without the intervention of some form of a sophisticated control logic such as HIS.

Chapter 9 provides a summary of this thesis with concluding remarks as well as an outlook towards future research.
1. Introduction
CHAPTER 1

System Overview

Content

2.1 UMTS ................................................................................................................................. 7
2.2 IEEE 802.11 .................................................................................................................... 30

Keywords: System Overview, Scanning Procedures, Synchronization, Measurements

The following chapter provides an overview of UMTS and IEEE 802.11. The scope, however, is not to give an enclosing system description, but to concentrate on means that support synchronization and acquisition of measurements. The Hybrid Information System as introduced later on in Section 5, relies on standard conformant (intra-system) measurements, gathered by legacy terminals. It is important to underline, that existing specifications dispose of a number of means to reflect the current system state. Exploitation and disposition of actually system restricted link state information to support system integration/cooperation is the actual benefit behind the concept.

It will be shown, that some of the presented mechanisms and procedures, e.g., synchronization or compressed mode application, are rather complex. Dedicated investigations in the analysis and simulation chapter will disclose drawbacks because of state-of-the-art information gathering by means of self-conducted scanning. Cognition of existing mechanisms as described in the following is the basis to understand the concept of the Hybrid Information System.

2.1 UMTS

The Universal Mobile Telecommunications System (UMTS) is one of the mobile radio specifications that have been taken up by the International Telecommunications Union (ITU) as member of the IMT-2000 (International Mobile Tele-
communications at 2000 MHz) family. IMT-2000 compatible systems are required to fulfill well-defined requisitions such as high bit rates (144 kbit/s – 2 Mbit/s), symmetric and asymmetric transmission, circuit and packet switched transmission, high quality for speech services and high spectrum efficiency [124].

Initially, the *European Telecommunications Standards Institute* (ETSI) was responsible for the UMTS standardization process. To allow for worldwide-harmonized specifications, the *Third Generation Partnership Project* (3GPP) was formed in 1998 to take over and continue the technical specification work. To meet new market requirements, 3GPP specifications are continually being enhanced. New aspects that are considered are referred to as ‘features’. In order to provide developers with a stable platform for implementation while at the same time allowing for development of new capabilities, a system of parallel ‘releases’ is applied. Initial UMTS deployments mainly apply the *Release 99* (R99). With R4, QoS support for the core network is an important new aspect and R5 introduces an entirely new core network concept based on IP. This will be further enhanced with R6 resulting in the circuit switched domain entirely replaced by the packet switched domain. An important enhancement within future releases is *Location Services* (LCS). A more detailed description on UMTS LCS together with benefits arising from application of concepts of this thesis is presented in Section 5.6.1.

**Figure 2.1: UTRA architecture of the access stratum**
Figure 2.2: UTRA protocol stack at Uu [157]

The UTRA architecture of the access stratum is shown in Figure 2.1. The Core Network (CN) part is further divided into a Circuit Switched Domain (CSD) domain and a Packet Switched Domain (PSD). Elements of the CSD comprise the Mobile Switching Center (MSC), Home Location Register (HLR), and Visitor Location Register (VLR). While the MSC is responsible for routing, circuit switching, location support, and handover, the two location registers administer user specific information. Elements of the PSD comprise the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). The SGSN performs similar tasks in the PSD like the MSC in the CSD but using packet switching. The GGSN serves as termination point of IP-tunnels and accomplishes context transfer actions. Two further entities, finally, the Equipment Identity Register (EIR) and the Authentication Center (AuC) that interact both, with PSD and CSD, round off the CN part of UMTS.

For the Radio Network Subsystem (RNS) as shown in Figure 2.1, there are two entities to be mentioned: The Radio Network Controller (RNC) and the Node B. The latter is responsible for radio transmission in one or more cells. The RNC is responsible for management and controlling functions including resource allocation, scheduling, and handover.

The User Equipment (UE) finally is the corresponding mobile entity being used by the customers.
The air interface between the UE and the RNS is referred to as $U_{u}$. Figure 2.2 depicts the respective protocol stack. Since Node B is involved in Layer 1 tasks, many protocol aspects related to the PHY will be implemented here. Accordingly, tasks related to RRC, but also RLC and MAC will be realized within the RNC.

A detailed description of all these entities and interfaces is not possible within this thesis. For more profound information, please refer to [157] providing a comprehensive description of UMTS entities including analytical and simulative traffic performance figures.

2.1.1 General Overview

In addition to satellite-based communication, which will not be addressed further within this work, UMTS specifies *UMTS Terrestrial Radio Access* (UTRA) together with an entire *UMTS Radio Access Network* (UTRAN). The underlying basic access scheme is *Wideband Code Division Multiple Access* (WCDMA), on top of which two duplex schemes have been specified: *Frequency Division Duplex* (UTRA-FDD) and *Time Division Duplex* (UTRA-TDD). These two operation modes differ in the applied duplex technique and multiple access scheme. While the physical layer specifications address specific properties of these operation modes, higher layer protocols and system components are almost the same.

![Figure 2.3: General UMTS Frame Structure for TDD and FDD](image)

Both schemes, UMTS-FDD and UMTS-TDD, are based on the same frame structure with a radio frame length of 10 ms as shown in Figure 2.3. The basic
information unit in UMTS is 1 chip. A frame thereby covers the time span needed to transmit 38400 chips. Accordingly, the resulting chip rate is 3.84 Mchip/s\(^1\). Each frame is further divided into 15 time slots, each carrying 2560 chip. The chip duration \(T_{\text{chip}}\) corresponds to 0.2604 \(\mu\)s.

### 2.1.1.1 UTRA-FDD

UTRA-FDD applies the *Code Division Multiple Access* (CDMA) scheme as shown in Figure 2.4. Different users, respectively physical channels, are distinguished by dedicated codes. Multiple users simultaneously transmit data using the same frequency band but with different spreading and scrambling\(^2\) codes. Accordingly, the underlying slotted time scheme with frames and time slots is not used to achieve separation of user signals but serves for realization of periodically occurring functions such as power control. Transmission of user data typically corresponds to a multiple of the frame duration. Thus, a user allocates all slots of one or more succeeding radio frames.

![Figure 2.4: Multiple Access in UTRA-FDD](image_url)

UTRA-FDD defines spreading factors of 4 - 512 (\(2^n\) with \(n = 2, 3, \ldots, 9\)) for downlink direction and 4 - 256 (\(2^n\) with \(n = 2, \ldots, 8\)) for uplink direction. If an

---

\(^1\) For the sake of completeness, it is to mention that UTRA-TDD specifies an additional physical layer scheme with 1.28 MChip/s [3].

\(^2\) Different scrambling codes only in uplink direction.
operator is allowed to use more than one single frequency band, *Frequency Division Multiple Access* (FDMA) may be used in addition to CDMA. The entire set of spreading codes may thereby be re-used in each band. In literature, spreading codes are also referred to as *channelization codes*. Both notations are used synonymously.

### 2.1.1.2 UTRA-TDD

UTRA-TDD uses the same frequency band for uplink and downlink direction. Each frame covers at least one time slot for uplink and one time slot for downlink transmission. The choice of the so-called *switching point*, which denotes switching from DL to UL and vice versa, is not predetermined by the UMTS specification. Instead, it may be arbitrarily chosen according to specific needs. A detailed investigation of this topic is presented in [4]. Contrary to UTRA-FDD, a physical channel is characterized not only by the spreading code but also by the time slot. Due to combination with CDMA, several physical channels may be realized simultaneously within one single time slot, see Figure 2.5.

![Figure 2.5: Multiple Access in UTRA-TDD](image)

While transmissions in UTRA-FDD span one or more succeeding time slots or even frames, physical channels in UTRA-TDD usually are restricted to one single time slot per frame. This in turn means that only reduced spreading factors of
1 - 16 can be applied if bit rates comparable to UTRA-FDD are to be achieved since the nominal symbol rate (3.84 Mchip/s) is the same as in UTRA-FDD.

Similar to UTRA-FDD, UTRA-TDD may use FDMA in addition to CDMA if the operator disposes of several frequency bands. A summary of the most important UMTS-TDD and -FDD characteristics is provided in Table 2.1.

Table 2.1: Summary of UMTS FDD/TDD characteristics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>UTRA FDD</th>
<th>UTRA TDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplex Scheme</td>
<td>FDD</td>
<td>TDD</td>
</tr>
<tr>
<td>Multiple Access Scheme</td>
<td>CDMA/FDMA</td>
<td>CDMA/FDMA/ TDMA</td>
</tr>
<tr>
<td>Spreading Factor UL</td>
<td>4 - 256</td>
<td>1 - 16</td>
</tr>
<tr>
<td>Spreading Factor DL</td>
<td>4 - 512</td>
<td>1 or 16</td>
</tr>
<tr>
<td>Scrambling</td>
<td>station specific</td>
<td>cell specific</td>
</tr>
<tr>
<td>Time Slots/Frame UL</td>
<td>15</td>
<td>1-14 (of 15)</td>
</tr>
<tr>
<td>Time Slots/Frame DL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modulation</td>
<td></td>
<td>QPSK</td>
</tr>
<tr>
<td>Frame Duration</td>
<td></td>
<td>10 ms</td>
</tr>
<tr>
<td>Symbol Rate</td>
<td></td>
<td>3.84 Mchip/s</td>
</tr>
</tbody>
</table>

2.1.2 Synchronization & Cell Search

Any service to be used requires prior synchronization of the mobile to the network with subsequent detection of the applied scrambling code. The scrambling code allows for quasi-orthogonal coding of cells in downlink direction and users in uplink direction. It thus represents a kind of Cell Id/User-Id, which helps to distinguish different communication partners. Quasi-orthogonality is an important characteristic to cope with problems arising from asynchronous signals. Due to run-time inherent delays, orthogonality of different signals is no longer guaranteed. Scrambling codes help to preserve a high degree of orthogonality (= quasi orthogonality) due to their robustness against time shifts.

UTRA-FDD specifies station specific scrambling codes. Accordingly, each base station and each mobile station uses a different scrambling code. UTRA-TDD,  

---

3 This holds only for a specific geographic area with possible interference impacts. Cells/terminals beyond the frequency re-use distance obviously will apply similar scrambling codes.
however, specifies cell specific scrambling codes. For the latter, all terminals in a cell use the same scrambling code as the base station. As a basic principle, neighboring base stations in UTRA-TDD and FDD always apply different scrambling codes. For this, data streams in downlink direction are always (quasi) orthogonal.

To allow for communication in either UMTS-FDD or -TDD, the first step is to figure out the applied scrambling code in the cell. The following subsections describe the cell search procedure for both UTRAN operation modes. The basic procedure is rather similar: By evaluation of dedicated synchronization channels, initial slot/frame synchronization is achieved. The subsequent derivation of the cell’s code group further cuts down the number of possible scrambling codes. Finally, a trial and error phase follows in which all codes according to the detected code group are tested.

One can anticipate that the cell search procedure is a complex and time-consuming task. If the UE has received information on which cell parameters or SCH configurations to search for, cell search can be considerably simplified. The Hybrid Information System as proposed in the scope of this thesis, see Section 5, will meet these challenges in the context of vertical handover control.

2.1.2.1 UTRA-FDD

Synchronization in UTRA-FDD as described in [5] is done stepwise. After initial switch-on, a terminal firstly needs to synchronize to the given time slot scheme (step 1), see Figure 2.6. Once the slot structure is known, frame synchronization and code-group identification is done afterwards (step 2). The next step is to determine the applied downlink scrambling code (step 3), which is necessary to receive further system information (step 4) being provided on scrambled channels only.
In the following, the different steps of the cell search procedure in UTRA-FDD are explained in more detail.

**Step 1: Slot Synchronization**
The first step is to use the *Primary Synchronization Code* (PSC) of the *Primary Synchronization Channel* (P-SCH) to acquire slot synchronization to a cell. The PSC is a code of 256 Chips length. It is common to all cells and repeated at the beginning of each slot, see Figure 2.7. The slot timing can be obtained by detecting peaks in a matched filter output.

**Step 2: Frame Synchronization and Code-Group Identification**
During the second step of the cell search procedure, the UE uses the *Secondary Synchronization Code* (SSC) of the *Secondary Synchronization Channel* (S-SCH). The S-SCH conveys a specific symbol sequence representing one out of sixty-four code groups. One code group thereby is represented by a sequence of 16 symbols (S1-S16). Since the cyclic shifts of the sequences are unique, the code group as well as the frame synchronization is determined.

An example is given in Table 2.2: Assuming a terminal receives the symbol sequence S15, S5, S5, S12, S16, it can directly derive that the applied primary scrambling code is part of code-group CG3. Furthermore, it can determine that the current slot number is four; ergo the frame start time was three slots earlier. This is how frame synchronization and code-group identification is achieved.
Table 2.2: Use of S-SCH for Frame Synchronization & Code Group identification

<table>
<thead>
<tr>
<th>Scrambling Code Group</th>
<th>Time Slot Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>CG1</td>
<td>S1</td>
</tr>
<tr>
<td>CG2</td>
<td>S1</td>
</tr>
<tr>
<td>CG3</td>
<td>S1</td>
</tr>
<tr>
<td>CG4</td>
<td>S1</td>
</tr>
<tr>
<td>CG5</td>
<td>S1</td>
</tr>
<tr>
<td>CG63</td>
<td>S9</td>
</tr>
<tr>
<td>CG64</td>
<td>S9</td>
</tr>
</tbody>
</table>

Step 3: Scrambling Code Identification
The determined code group identifier represents eight scrambling codes, one of which is applied in the current cell. To figure out which of these codes is the right one, a ‘trial and error’ approach is applied for the scrambled Common Pilot Channel (CPICH): The primary scrambling code is typically identified through symbol-by-symbol correlation over the CPICH with all eight codes within the code group identified in the second step.

Step 4: Retrieval of System Information
Once the applied downlink scrambling code is known, the Primary Common Control Physical Channel (P-CCPCH) can be detected and the system- and cell specific Broadcast Channel (BCH) information can be read. Whenever a user wants to start a service, e.g., making a phone call, the respective spreading codes for uplink and downlink as well as the user identification scrambling code for the uplink are reported via special channels. The BCH provides information which channels respectively codes are to be used to get this system information.

2.1.2.2 UTRA-TDD
Synchronization and cell search in UTRA-TDD follow the same principle as in UTRA-FDD, see Figure 2.6. Since the underlying frame and slot structure as shown in Figure 2.3 is valid for both operation modes, the respective steps as presented in the previous section in principle apply for UTRA-TDD, too. However, due to different burst types used in UTRA-TDD, additional parameters such as the basic midamble code need to be figured out. Furthermore, time off-
sets $t_{\text{offset},n}$ have been introduced to overcome capture effects of the SCH arising from synchronous operation of neighboring base stations.

In detail, the following steps need to be executed:

**Step 1: Primary Synchronization Code Acquisition**

Similar to UTRA-FDD, the first step is to evaluate the *Primary Synchronization Code* (PSC) on the Synchronization Channel (SCH). This is typically done with a single matched filter, matched to the 256 chips long PSC which is common to all cells. A cell can be found by detecting peaks in the filter’s output. In order not to limit the uplink/downlink asymmetry, the SCH is mapped on one (case 1) or two (case 2) downlink slots per frame, see Figure 2.7. Accordingly, the SCH can be received periodically every 15 slots (case 1) or with offsets of either 7 or 8 slots (case 2) from the previous SCH transmission.

**Step 2: Code Group Identification & Slot Synchronization**

During the second step of the cell search procedure, the UE uses the SCH's secondary synchronization codes to identify 1 out of 32 code groups for the cell found in the first step. This is typically done by correlating the received signal with the secondary synchronization codes at the detected peak positions of the first step. The primary synchronization code provides the phase reference for coherent detection of the secondary synchronization codes. The code group can then uniquely be identified by detection of the maximum correlation values.

Each code group indicates a different $t_{\text{offset}}$ parameter and four specific cell parameters. Each of the cell parameters is associated with one particular downlink scrambling code and one particular long and short basic midamble code. When the UE has determined the code group, it can unambiguously derive the slot timing of the discovered cell from the detected peak position in the first step and the $t_{\text{offset}}$ parameter of the found code group in the second step.

**Step 3: Downlink Scrambling Code & basic Midamble Code Identification**

During the third and last step of the cell search procedure, the UE determines the exact downlink scrambling code, basic midamble code, and frame timing used by the discovered cell. The long basic midamble code can be identified by correlation over the P-CCPCH with the possible four basic midamble codes of the code group found in the second step.
Figure 2.7: Primary and Secondary Synchronization Channel in UTRA-FDD/-TDD

The position of the P-CCPCH is inherently known from the SCH reception in step 1. For case 1, P-CCPCH and SCH are transmitted simultaneously, for case 2, the P-CCPCH is transmitted together with the first SCH in a frame. When the long basic midamble code has been identified, downlink scrambling code and cell parameter are known.

Step 4: Frame Synchronization & Retrieval of System Information
Once the applied downlink scrambling code is known, the UE can read system- and cell-specific BCH information and acquire frame synchronization.
Summarizing this, one can see that the determination of applied code sequences is required for synchronization in both, UTRA-FDD and UTRA-TDD. Table 2.3 subsumes respective properties.

**Table 2.3: Synchronization/Scrambling Codes for UTRA-FDD/TDD**

<table>
<thead>
<tr>
<th></th>
<th>UTRA-FDD</th>
<th>UTRA-TDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Synchronization Code (PSC)</td>
<td>1x 256 chip</td>
<td>Common to all cells</td>
</tr>
<tr>
<td></td>
<td>15 times / frame</td>
<td>1-2 times / frame</td>
</tr>
<tr>
<td># Secondary Synchronization Codes (SSC)</td>
<td>16 x 256 chip</td>
<td>12 x 256 chip</td>
</tr>
<tr>
<td># Scrambling Code Groups</td>
<td>64</td>
<td>32</td>
</tr>
</tbody>
</table>

### 2.1.3 Scanning of Complementary Systems & Compressed Mode

A basic requirement for interoperability between UMTS and other radio systems is the possibility to detect and survey other networks. TDMA/TDD systems like the *Global System for Mobile Communications* (GSM) or dedicated *Wireless Local Area Networks* (WLAN) that are based on separation of users in the time domain allow the terminal to perform measurements within idle slots. The WLAN HIPERLAN/2 further specifies an absence procedure during which a terminal is temporary unavailable in order to perform measurements on neighboring cells [14]. However, during this time, no communication between the terminal and the current AP is possible.

For UMTS, which supports both, TDD and FDD operation, a respective distinction needs to be done: Due to the slotted access in TDD, scanning of other frequencies, the other mode or another radio access technology is easily feasible during idle slots and therefore similar mechanisms as for other time based separated systems apply.

Against this, the FDD mode with its continuous and parallel reception and transmission scheme, does not offer inherent idle periods that allow the mobile intermediate switching to other frequencies for scanning. To overcome this problem, different solutions may be applied, such as:

- a second receiver for scanning
- installation of a single wide-band receiver
- establishment of a quasi-continuous transmission/reception scheme
However, the proposed solutions imply some drawbacks: A second receiver directly affects design characteristics like prize, size, or power consumption. If a one-transceiver solution shall be designed, a possible realization would be the usage of a single wide-band receiver scanning the entire contemplable band. However, this solution suffers from high challenges, e.g., with respect to the supported dynamic range, sensitivity and filters. Therefore, the third possibility is the one being specified for UMTS-FDD.

By establishing a quasi-continuous transceiver scheme, the continuous reception and transmission in FDD mode is adapted to allow for scanning during exclusively generated idle time slots. One constraint thereby is that the supplied data or speech service shall be maintained with as less restrictions as possible. The applied realization scheme is referred to as Compressed Mode (CM).

2.1.3.1 Realization of Compressed Mode

Compressed Mode is defined as the mechanism whereby certain idle periods are created in radio frames so that the UE can perform measurements during these periods [64]. Another denotation for ‘idle periods’ is Transmission Gap (TG). A TG is made up of consecutive empty slots that have been obtained with a transmission time reduction method. The total Transmission Gap Length (TGL) amounts between 0 and 14 slots, whereby the TG can be contained in one (single frame method) or two (double frame method) consecutive radio frames. The maximum TGL in one single frame is limited to 7 slots. When in compressed mode, the information normally transmitted during a 10 ms frame is compressed in time. The mechanisms provided for achieving this are:

1) Puncturing: UMTS applies rate matching by repeating or puncturing bits in the transport channel to fit in a physical channel. In the case of bit-repetition, e.g., 12.2 kbps for speech in UTRA-FDD, the amount of data can easily be reduced by puncturing of redundant bits. This is how rate matching allows for creation of TGs in one or two frames. The algorithm for rate matching is specified in [15].

2) Higher Layer Scheduling: Another possibility for achieving CM is the disposition of data e.g., in terms of scheduling by higher layers. By setting restrictions, only a subset of the allowed Transport Format Combinations (TFC) is used. Hence, the amount of data for the physical layer is known and an idle gap can be generated.
3) Reducing the spreading factor: The third method for CM as specified for UMTS is to reduce the spreading factor during one compressed radio frame, which allows for transmission of the information bits within a shorter period. Since the resulting signal is less robust, transmission power needs to be increased simultaneously. On the downlink, UTRAN can also order the UE to use a different scrambling code in a compressed frame than in a non-compressed frame.

All these methods are depicted in Figure 2.8. In the downlink, all methods are supported while compressed mode by puncturing is not used in the uplink.

![Figure 2.8: Compressed Mode transmission in UTRA-FDD](image)

Compressed Mode is obtained by layer 2 using transport channels provided by the layer 1. Control is managed by the RRC layer, which configures the layer 2 and the physical layer. The UE shall support a total number of simultaneous compressed mode pattern sequences, depending on its capability to support different measurement types as presented in Section 2.1.4.1. For example, a UE

---

4 The presented approaches for TG generation are related to L1/L2 point of views and refer to legacy ‘non-intelligent’ transmission techniques. In fact, resulting bitstreams of services/applications inherently dispose of short breaks or can at least tolerate delays. Considering these natural discontinuities could relax the necessity for mechanisms due to Figure 2.8. An underlying intelligent scanning scheduler hence needs to consider the respective services in its TG generation.
supporting FDD and GSM shall support four simultaneous compressed mode pattern sequences and a UE supporting FDD and TDD shall support two simultaneous compressed mode pattern sequences [64].

Unlike absence procedures that result in effective disconnection with service interruption, the compressed mode aims on establishing quasi-continuous operation. Thereby, the same information bit-rate as in normal operation is conveyed, but the actual transmission occurs only during a fraction of the radio frame. Transmission gaps thus are realized by compressing the data stream during a few slots.

An inherent drawback thereby is that further control measures become necessary. As illustrated in Figure 2.8b, the instantaneous transmit power is increased in the compressed frame in order to keep transmission quality (BER, FER, etc.) unaffected by the reduced processing gain. The amount of power increase depends on the transmission time reduction method. Further, the decision on which frames are compressed is taken by the network. Applying compressed mode, compressed frames can occur periodically or they can be generated on demand. The rate and type of compressed frames is variable and depends on the environment and the measurement requirements.

Besides facilitation of scanning due to created TGs, the compressed mode is further applied to support functions such as HO preparation by information exchange/signaling with a new target base station during a transmission gap. Accordingly, different types of frame structures are defined for downlink compressed frames. Type A maximizes the transmission gap length and type B is optimized for power control. The frame structure type A or B is set by higher layers.

One can imagine, that implementation, application and control of CM procedures is a complex task. However, up to now, alternative means of making the measurements are not yet considered within 3GPP.

Within the scope of this thesis, initial investigations with respect to CM performance have been undertaken with partial publication in [65]. All results are presented in Section 8.2.2. It will be shown that CM is not just a non-preferable means to gather system information, but it has even a negative impact on the overall system performance of UMTS.

A logical consequence thus is to conceive alternative concepts of information gathering, making CM application obsolete or less frequently used. The Hybrid Information System as presented in Section 5 is one such promising approach.
2.1.4 Measurements in UMTS

The initial UE cell search procedure for UTRA-FDD and UTRA-TDD after switching on has been described in Section 2.1.2. Since different Public Land Mobile Networks (PLMNs) may be available for service provisioning, internal preferences need to be followed. The selection of the particular PLMN to be contacted may be carried out either automatically or manually. The related Non-Access-Stratum (NAS) functions for mobile stations in idle mode have been specified by 3GPP in [7]. The NAS provides a list, if available, of equivalent PLMNs that the Access Stratum (AS) shall use for cell selection and cell reselection. The UE searches for a suitable cell of the chosen PLMN and tunes to its control channel. This procedure is known as ‘camping on the cell’ [8]. The UE will then register its presence by means of a NAS registration procedure. If necessary, the UE shall search for higher priority PLMNs at regular time intervals between 6 minutes and 8 hours, with a step size of 6 minutes as described in [9] and search for a suitable cell if another PLMN has been selected by NAS. The plain idle mode cell selection and reselection procedure is shown in Figure 2.9 [8]. In any case, a new PLMN selection causes an exit to number 1.

![Diagram of Idle mode cell selection & re-selection with economy potential](image)

Figure 2.9: Idle mode cell selection & re-selection with economy potential

‘Initial Cell Selection’, cp. Figure 2.9, requires an entire scan of all RF channels in the UTRA bands to find available PLMNs. On each carrier, the UE needs to
search for the strongest cell and reads transmitted system information as described in Section 2.1.2, in order to find out to which PLMN the cell belongs. If dedicated information of carrier frequencies and cell parameters, e.g., scrambling codes, are available, the UE may optimize the cell search by applying the ‘Stored information Cell Selection’ procedure, see Figure 2.9. The Hybrid Information System as to be introduced within Section 5 precisely aims on providing respective data. Thus, direct application of the improved cell selection method is facilitated making time-consuming Initial Cell Selection procedures obsolete.

2.1.4.1 Physical Layer Measurements

The Radio Network Controller (RNC) as introduced in Section 2.1 is the central node of the UMTS Radio Access Network (UTRAN). It takes over tasks such as resource control including channel allocation, handover, and power control. For this, major parts of the protocols between UE and RAN are implemented here. In order to perform optimal control, the RNC-RRC entity relies on dedicated measurements of the physical layer. A specific interface allows for direct information exchange between L1 and L3, skipping L2 as shown in Figure 2.10. Communication is performed in an abstract way by means of CPHY-primitives.

![Figure 2.10: Interfaces with the Physical Layer [64]](image)

Measurements of the physical layer are used to trigger or perform a multitude of functions. Both the UE and the UTRAN are required to perform a variety of measurements. The standard does not specify the method to perform these measurements or stipulate that the list of measurements within [64] must all be performed. While some of the measurements are critical for functioning of the network and are mandatory for delivering the basic functionality (e.g., handover
measurements, power control measurements), others may be used by the network operators for optimizing the network (e.g., radio environment).

A general overview of measurements within UMTS offered by layer 1 is provided in [64]. The UE physical layer measurements, based on which cell (re-)selection, handover, dynamic channel allocation and timing advance are controlled, are described in [10] for UTRA-FDD and [11] for UTRA-TDD. Feedback signaling to the UTRAN is realized with special measurement reports, which may be generated on request or spontaneously. Compilation of measurement reports in UMTS is described in more detail in Section 2.1.5.

As discussed, measurements are distinguished between measurements in the UE and measurements in the UTRAN. Table 2.4 summarizes the entire measurement abilities as specified for the physical layer in [10] and [11]. Corresponding measurements on either network element respectively operation mode have been ordered in one row for direct comparison. Since it is not possible to describe the purpose of each measurement in detail, it is herewith referred to the specifications [10] and [11]. However, some measurements are self-explanatory anyway; others will be partly referred to later on if necessary. Since not all measurements are defined as mandatory, the UMTS specification defines so-called UE capabilities, which are reported to the network during the association procedure or on request.

**Table 2.4: Measurement capabilities specified by UTRA TDD/FDD**

<table>
<thead>
<tr>
<th>UTRA TDD</th>
<th>UTRA FDD</th>
<th>UTRA TDD</th>
<th>UTRA FDD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UE</strong></td>
<td><strong>UTRAN</strong></td>
<td><strong>Signal Power</strong></td>
<td></td>
</tr>
<tr>
<td>P-CCPCH RSCP</td>
<td></td>
<td>Transmitted carrier power</td>
<td></td>
</tr>
<tr>
<td>CPICH RSCP</td>
<td></td>
<td>Transmitted code power</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UE transmitted power</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UTRA carrier RSSI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GSM carrier RSSI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmitted carrier power of all codes not used for HS-PDSCH or HS-SCCH transmission</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UTRA TDD</td>
<td>UTRA FDD</td>
<td>UTRA TDD</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>UE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>UTRAN</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Interference Power</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time slot ISCP</td>
<td></td>
<td>Time slot ISCP</td>
<td></td>
</tr>
<tr>
<td>UpPTS interference (1.28 Mcps TDD)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Received total wide band power</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ratios of Signal and Interference Power</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIR</td>
<td>SIR</td>
<td></td>
<td>SIR, SIR&lt;sub&gt;error&lt;/sub&gt;</td>
</tr>
<tr>
<td>CPICH Ec/No</td>
<td></td>
<td></td>
<td>Cell Sync Burst SIR</td>
</tr>
<tr>
<td><strong>Observed Error Rates</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport channel BLER</td>
<td></td>
<td></td>
<td>Transport channel BER</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HS-SICH reception quality</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Physical channel BER</td>
</tr>
<tr>
<td><strong>Observed Timing</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFN-SFN observed time difference</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observed time difference to GSM cell</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SFN-CFN observed time difference</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UE GPS code phase</td>
<td></td>
<td></td>
<td>Cell Sync Burst Timing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RX Timing Deviation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UE Rx-Tx time difference</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Received SYNC-UL Timing Deviation for 1.28 Mcps TDD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Round trip time</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PRACH/PCPCH Propagation delay</td>
</tr>
<tr>
<td>Timing Advance (TADV) for 1.28 Mcps TDD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Localization Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Angle of Arrival (AoA) for 1.28 Mcps TDD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UE GPS Timing of Cell Frames for UE</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.1. UMTS

While execution of these measurements shall partly be done in parallel by the UE, it is required in [12] that each measurement is controlled and reported independently of any other.

Cells that the UE is monitoring are grouped in the UE into three mutually exclusive categories:

1. **Active set**: Cells that provide user information. In FDD, the cells in the active set are involved in soft handover. In TDD, the active set always comprises one cell only.

1. **Monitored set**: Cells, which are not included in the active set, but are included in the CELL_INFO_LIST, belong to the monitored set.

3. **Detected set**: Cells detected by the UE, which are neither in the CELL_INFO_LIST nor in the active set, belong to the detected set.

In general, measurements can be differentiated in different measurement types [12]:

- **Intra-frequency measurements**: Measurements on downlink physical channels at the same frequency as the active set. A measurement object corresponds to one cell.

- **Inter-frequency measurements**: Measurements on downlink physical channels at frequencies that differ from the frequency of the active set.
and on downlink physical channels in the active set. A measurement object corresponds to one cell.

- **Inter-RAT measurements**: Measurements on downlink physical channels belonging to another radio access technology than UTRAN, e.g., GSM. A measurement object corresponds to one cell.

- **Traffic volume measurements**: Measurements on uplink traffic volume. A measurement object corresponds to one cell.

- **Quality measurements**: Measurements of downlink quality parameters, e.g., downlink transport block error rate. A measurement object corresponds to one transport channel in case of BLER. A measurement object corresponds to one time slot in case of SIR (TDD only).

- **UE-internal measurements**: Internal measurements of UE transmission power and UE received signal level.

- **UE positioning measurements**: Measurements of UE position.

As shown in Table 2.4, UMTS specifies dedicated measurements for positioning support. The underlying concept of the Hybrid Information System as presented in Section 5 relies on location specific measurement reports, i.e., measurements as reported by UEs are associated with respective position information.

### 2.1.5 Measurement Reports

To initiate a specific measurement the UTRAN transmits a ‘measurement control message’ as specified in [12] to the UE including a measurement ID, a command (setup, modify, release), and a measurement type. In idle mode, the measurement control message is broadcast as *System Information*. Presence or absence of control elements depends on the associated measurement type. In detail, these are measurement objects, reporting quantities and -criteria (periodical/event-triggered) and mode (acknowledged/unacknowledged). In addition, measurement validity defines in which UE states the measurements are valid.

Measurements may be performed and reported periodically to the upper layers, or they may be generated on an event-triggered basis (e.g., a new primary
CCPCH exceeds a previous best primary CCPCH). Another reporting strategy may combine the event triggered and the periodical approach (e.g., falling of link quality below a certain threshold initiates periodical reporting). In addition, measurements in the UE may explicitly be requested by the network.

**Figure 2.11: Measurement Report procedure in UMTS**

Figure 2.11 illustrates the latter case: As described in Section 2.1.4.1, the RNC needs to gather information on the current system state. For this, it advices the UE to carry out specific measurements with a MEASUREMENT CONTROL message. On reception of the request, the UE-RRC instructs its physical layer to carry out the requested measurements by sending a CPHY-Measurement-REQ. The physical layer hereafter initiates respective measurements. How the measurements are actually executed by an implementation is not constrained by the standard, i.e., the model does not state a specific sampling rate or even if the sampling is periodic or not [64]. The same holds for possible L1 filtering. What the standard specifies in [62] for UTRA-TDD [63] UTRA-FDD is the performance objective and measurement period from L3 perspective as well as L3 filtering to be applied. Once previously defined reporting criteria are fulfilled, the UE-RRC generates a MEASUREMENT REPORT, which is transmitted back to the network.
2.2 IEEE 802.11

The following section provides an overview of the Wireless Local Area Network (WLAN) 802.11 according to specifications of IEEE. In contrast to cellular mobile radio systems such as UMTS, WLAN focus on coverage support for Small Office/Home Office (SoHo) environments. Within the last years, the concept was expanded to limited outdoor deployment for so-called Hot Spot areas, e.g., airports, market places or university campuses. In parallel to IEEE 802.11, other WLAN specifications have been developed such as HIPERLAN/2 [13], but the enormous economic success of IEEE 802.11 with its worldwide penetration made it a de facto standard for wireless LAN systems.

However, being initially developed for SoHo environments, widespread WLAN application introduced new challenges. Enhanced requirements with respect to security, QoS support and increased data rates led to standard amendments by dedicated task groups. Within most of these enhancements, focus was put on standard inherent improvements. According to its original specification as pure access technology, only the lower two layers are addressed by 802.11. This lead to a neglect of interworking properties failed to be anchored in the standard. Meanwhile, it was realized that system integration and cooperation is not only subject to higher layers.

To cope with these requirements, new mechanisms and amendments for L2/L1 based information provisioning have been derived or are under investigation within IEEE. Description of related measurements is the focus of this chapter. After a short general overview of IEEE 802.11 in Section 2.2.1, a description of legacy synchronization and scanning procedures is given in Sections 2.2.2 and 2.2.3. Section 2.2.4 explains the regulatory framework for exchange of measurement information. Section 2.2.5 explains comprehensively specific measurements according to 802.11h. More details on further related specifications, namely 802.11k, have been taken up in the annex.

2.2.1 General Overview

IEEE 802.11 denotes a family of Wireless Local Area Network (WLAN) standards developed by working group 11 of the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). Like IEEE
802.3 (Ethernet) and IEEE 802.5 (Token Ring), 802.11 is restricted to the lower two layers of the ISO/OSI reference model [84], cp. Figure 2.12. The original version of the standard IEEE 802.11 was completed in 1997. A revised version wherein redundant management items had been removed, with enhanced appendices and minor modifications throughout the document was released in 1999 and re-affirmed as ANSI/IEEE Std 802.11, 1999 Edition (R2003) in 2003 [67]. The original 802.11 specifications sometimes are also referred to as legacy 802.11. Another denotation often used for the WLAN 802.11 family is Wireless Fidelity (WiFi). Certified products can use the official WiFi logo, which indicates that the product is interoperable with any other product showing the logo. Especially the interoperability aspect was one reason for which IEEE 802.11 became the worldwide leading standard for WLAN deployed mainly to cover SoHo and Hot Spot areas.

![Figure 2.12: ISO/OSI reference model [84] and IEEE 802.11 [86]](image)

The basic access method applied is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA serves as foundation of the IEEE 802.11 specific Distributed Coordination Function (DCF), which will be shortly explained in the next paragraph. DCF application allows for contention-based non-centralized medium access. Contention free access, centrally controlled by one single station, can be achieved by the Point Coordination Function (PCF) that resides on top of the DCF. However, in practice only few implementations of the PCF have been realized. A set of stations controlled by a single coordination function, either DCF or PCF, is referred to as Basic Service Set (BSS). A self-
contained BSS with no access to a Distribution System (DS) is called Independent Basic Service Set (IBSS). The term *ad hoc* is often used synonymously to refer to an IBSS.

Figure 2.13 depicts the basic DCF access method of 802.11. A station that wants to transmit data needs to monitor the medium prior to any access attempt. If the channel was found idle for a time span of at least DIFS (Distributed Coordination Function Interframe Space), an additional deferral time, the *random backoff period*, follows, before transmission is allowed. The aim thereby is to minimize collisions during contention between multiple stations. The duration of the random backoff is the product of the *Slot Time* and a uniformly distributed *pseudorandom integer*. The latter is drawn over the interval [0, CW], whereby CW (Contention Window) is within the range of values of the PHY characteristics $aCW_{min}$ and $aCW_{max}$, $aCW_{min} \leq CW \leq aCW_{max}$. Legacy 802.11 defines $aCW_{min} = 15(31)$ and $aCW_{max} = 1023$, while other standard amendments such as 802.11e [72] redefine these parameters as one means to support prioritization. Initial values for CW are chosen equal to $aCW_{min}$. Depending on consecutive delivery failures, the value for CW is drawn from sequentially ascending integer powers continuing up to a maximum value of $aCW_{max}$. If a station detects activity on the channel while still being in backoff countdown, the backoff procedure is suspended and not resumed unless another idle period of duration DIFS was measured.

![Figure 2.13: Basic access method of legacy 802.11](image)

In addition to DCF, legacy 802.11 incorporates some other mechanisms to optimize channel access and reliability of data transmission. For example, each correctly received frame is responded with a positive acknowledgement. Prioritized
channel access for the responding station thereby is achieved by a minimum waiting time of SIFS (Short Interframe Space). The earlier discussed PCF would acquire channel control by applying the waiting time PIFS (PCF Interframe Space) which is a bit longer than SIFS but shorter than DIFS. Other transmission properties of IEEE 802.11 target to support fragmented delivery of a single MAC Service Data Unit (MSDU). Further, a so-called Network Allocation Vector (NAV) defines a virtual carrier-sense mechanism in addition to CSMA-CA in order to prevent stations from accessing the medium.

Finally yet important, an expedient mechanism called Ready to Send (RTS) / Clear to Send (CTS) incorporating NAV is specified to mitigate the hidden node problem. A detailed description of these mechanisms is out of scope of this thesis. For more information, please refer to [67] or [157].

All time spans defined within 802.11 are based on the definition of SIFS and the Slot Time. Both of which in turn include further dependencies and are fixed for each specific PHY:

\[ aSIFSTime := aRxRFDelay + aRxPLCPDelay + aMACProcessingDelay + aRxTxTurnaroundTime \]  
\[ aSlotTime := aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay \]

Accordingly, PIFS and DIFS are derived by the following equations:

\[ PIFS := aSIFSTime + aSlotTime \]  
\[ DIFS := aSIFSTime + 2 \times aSlotTime \]

Table 2.5 gives an overview of durations according to legacy 802.11 and its amendments 802.11a, b and g.

Driven by the desire for more reliable, universal, and secure deployment, various amendments to legacy 802.11 have been specified or are under specification. Work is accomplished within special task groups labeled with alphabetical letters, e.g., Task Group a (TGa). Accordingly, the TG’s outcome i.e., the specification is referred to as 802.11a. On successfully passing a letter ballot, ratified specifications are published as supplement or amendment to the original legacy 802.11 specification.
The probably best-known amendment is IEEE 802.11b. An overview of important 802.11 TGs and specifications as of November 2005 is given in Table 2.6.

**Table 2.6: Properties of IEEE 802.11 supplements and amendments**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>Phy extension with max. 54 Mbit/s peak data rate, 5GHz band, 12 non-overlapping channels, Orthogonal Frequency Division Multiplexing (OFDM) Modulation</td>
<td>released: 1999 [69]</td>
</tr>
<tr>
<td>802.11b</td>
<td>Phy extension with max. 11 Mbit/s peak data rate, 2.4GHz band, 3 non-overlapping channels extension of DSSS modulation technique in the original standard</td>
<td>released: 1999 [71] Corrigendum 1: 2001</td>
</tr>
<tr>
<td>802.11c</td>
<td>Wireless Bridging between Access Points</td>
<td>completed, part ISO/IEC 10038 Standard (IEEE 802.1D)</td>
</tr>
<tr>
<td>802.11d</td>
<td>Specification for operation in additional regulatory</td>
<td>released: 2001</td>
</tr>
</tbody>
</table>

---

5 802.11, 1999 Edition Chapter 9.2.10 (DIFS=aSIFSTime + 2*aSlotTime), Table 57a (FH) and Table 59 (DS)
6 802.11a-1999, Table 93
7 802.11b-1999, Table 101
8 802.11g-2003, Table 123E and 123G
<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11e</td>
<td>QoS Enhancements&lt;br&gt;Prioritization of data packets</td>
<td>completed, waiting for approval of latest draft (Jan. 2005): 802.11e-D13.0 [72]</td>
</tr>
<tr>
<td>802.11F</td>
<td>Inter-Access Point Protocol (IAPP)&lt;br&gt;multi-vendor Access Point interoperability</td>
<td>released: 2003</td>
</tr>
<tr>
<td>802.11g</td>
<td>54 Mbit/s, 2.4 GHz standard (backwards compatible with 802.11b)&lt;br&gt;OFDM Modulation</td>
<td>released: 2003 [73]</td>
</tr>
<tr>
<td>802.11h</td>
<td>Radio Resource Management&lt;br&gt;Dynamic Channel/Frequency Selection (DCS/DFS)&lt;br&gt;Transmit Power Control (TPC)</td>
<td>released: 2003 [74]</td>
</tr>
<tr>
<td>802.11i</td>
<td>Enhanced security</td>
<td>released: 2004</td>
</tr>
<tr>
<td>802.11j</td>
<td>Extensions of 802.11 MAC and 802.11a for Japan, 4.9GHz - 5GHz</td>
<td>released: 2004</td>
</tr>
<tr>
<td>802.11k</td>
<td>Radio Resource Measurements&lt;br&gt;measurements and other information to manage services (externally)</td>
<td>work in progress&lt;br&gt;latest draft (Oct. ‘05): P802.11k-D3.0 [75]</td>
</tr>
<tr>
<td>802.11m</td>
<td>Maintenance, technical and editorial corrections</td>
<td>work in progress&lt;br&gt;latest draft (Sept 2005): P802.11-REVma-D4.0</td>
</tr>
<tr>
<td>802.11n</td>
<td>Higher throughput improvements, 108Mbit/s - 320MBit/s</td>
<td>work in progress&lt;br&gt;no draft available yet</td>
</tr>
<tr>
<td>802.11p</td>
<td>Wireless Access for the Vehicular Environment</td>
<td>work in progress&lt;br&gt;latest draft (Sept 2005) &lt;br&gt;P802.11p_D0.23</td>
</tr>
<tr>
<td>802.11r</td>
<td>Fast roaming and fast BSS transition</td>
<td>work in progress&lt;br&gt;latest draft (Sept 2005) &lt;br&gt;P802.11r-D0.09</td>
</tr>
<tr>
<td>802.11s</td>
<td>Wireless mesh networking</td>
<td>work in progress, no draft available yet (Sept. ‘05)</td>
</tr>
<tr>
<td>802.11t</td>
<td>Wireless Performance Prediction (WPP) - test methods&lt;br&gt;and metrics</td>
<td>work in progress, latest draft (Sept 2005) &lt;br&gt;P802.11.2-D0.3</td>
</tr>
<tr>
<td>802.11u</td>
<td>Interworking with non-802 networks (e.g., cellular)</td>
<td>work in progress, no</td>
</tr>
</tbody>
</table>
Due to the large range of activities covered by 802.11, it is not possible to describe each single task group within this thesis. Some groups even are still in their initial definition phase being subject to ongoing changes. Other groups have already released a standard amendment or have defined an adequately stable draft version. Two of them, 802.11h and 802.11k, are of particular interest in the scope of this work, for which they are explicitly pictured in the following subsections. Further TGs such as 802.11F and 802.11u are shortly addressed when talking about related work in the context of system integration.

An enclosing overview of different working groups characterized by their main field of activity is given in Figure 2.14 [78]. Further descriptions of 802 wireless systems including performance figures and spectrum coexistence have been compiled in [79].
2.2.2 Synchronization & Cell Search

Medium access in 802.11 is highly dependent on accurate timing functions. Specific time durations like SIFS, PIFS and DIFS as introduced in the previous section (see Figure 2.13) are the basis for ordered channel access. According to this, the specification states that all stations within a single BSS shall be synchronized to a common clock. A Timing Synchronization Function (TSF) hence is defined to allow for synchronization of local TSF timers. Each station maintains such a timer with modulus $2^{64}$ counting in increments of microseconds. This allows not just incremental but absolute scheduling of future tasks. In an infrastructure-based network, TSF is performed by the AP that serves as timing master. Independent basic service sets with no central control instance apply a distributed TSF algorithm. However, synchronization in IBSSs is beyond the scope of this thesis and not further considered.

To allow for synchronization of local TSF timers of stations within a BSS, the AP periodically transmits special frames called Beacons. In addition to general information on supported capabilities, Service Set Identification (SSID), supported rates, PHY parameter information and Traffic Indication Messages (TIM, DTIM), the two most important elements with respect to synchronization are a Timestamp and a Beacon Interval field. The 64-bit timestamp contains a copy of the AP’s TSF timer when transmitting the beacon. Internal processing delays
between layer 2 and layer 1 may be considered by an additional offset so that the overall mechanism targets to maintain the synchronization to within 4 μs plus the maximum propagation delay. On receiving beacon timestamps, associated stations shall always accept the timing information sent by the AP regardless of the own local timer.

In addition to the timestamp, the beacon interval field is of particular interest. It reports the number of time units between two target beacon transmissions. As shown in Figure 2.15, beacon transmission may be delayed due to busy medium. This is why 802.11 specifies Target Beacon Transmission Times (TBTT). If a beacon is delayed and cannot be sent at the actual TBTT_1, it will be conveyed as soon as the medium is idle. The next beacon will be scheduled at TBTT_2 = TBTT_1 + Beacon Interval. If the medium is busy at TBTT_2, a delayed beacon is sent again and the next one is scheduled for TBTT_3. If the medium is idle at that time, TBTT_3 and actual beacon transmission will coincide, regardless of any delayed previous beacon transmission. In principle, beacon intervals can comprise any time span between 1 TU (≈ 1ms) and $2^{16}$-1 TUs (≈ 67 s) with a granularity of time units.

![Figure 2.15: Target and actual Beacon transmission on a busy network](image)

However, the specification does not prescribe any particular period. Currently, commercial IEEE 802.11a,b,g access points usually are shipped with a default beacon interval of 100 ms.

With the definition of the TBTT, an absolute timeframe is established decoupling target beacon transmissions from current load. In practice, however, actual beacon transmission and target beacon transmission should coincide to allow for
deterministic reception of system information. For this reason, 802.11e introduced beacon protection, see Figure 2.15. Stations with a valid transmission opportunity (TXOP) are not allowed to transmit across the TBTT. Hence, prior to initiate any frame exchange, it is to check whether the entire transmission would be completed before the next beacon broadcast. Otherwise, the station needs to defer and transmit later on. More investigations on beaconing and its impact on system throughput in a heterogeneous system environment will be presented in Section 8.5.1.

Knowledge about TBTT allows associated stations to operate in power save mode. While being in Doze state, a station is not able to transmit or receive and consumes very low power only. Switching to the Awake state hence is only necessary for selected beacons. Traffic indication messages conveyed together with each beacon further inform on buffered MSDU for a particular station or upcoming multicast/broadcast messages. Depending on this information, a station may switch back to Doze state or stay awake for further actions.

2.2.3 Scanning Procedures in WLAN 802.11

IEEE 802.11 defines two scanning modes: Passive and Active scanning. The decision on which scanning mode shall be applied is taken by the Station Management Entity (SME). The SME is a layer-independent entity that may be viewed as residing in a separate management plane, cp. Figure 2.12. The exact functions of the SME are not specified by the standard. In general, this entity is responsible for tasks such as the gathering of layer-dependent status information from the various layer management entities and setting the values of layer-specific parameters [67]. Hence, the SME executes actions related to general system management. Using the MLME-SCAN.request primitive, it directs the MAC Layer Management Entity (MLME) to perform either passive or active scanning. Additional scanning directives like a dedicated (B)SSID, a channel list or timing constraints for scanning (MinChannelTime, MaxChannelTime) can be prescribed, too. Similarly to the beacon interval, scanning periods are not regulated by the specification. Upon completion of scanning, an MLME-SCAN.confirm is compiled to report all received BSS information back to the SME.
2.2.3.1 Passive Scanning

If passive scanning is requested, a station monitors each specified channel for a time span of at most $\textbf{MaxChannelTime}$. If no specific (B)SSID or channel list was requested by the SME, the station needs to survey each channel from the valid channel range for the appropriate PHY and carrier set. During the scanning, the station adds any received 802.11-beacon or probe response to its cached BSSID scan list.

Depending on the number of channels to be scanned, the Beacon Interval of a single BSS, the synchronicity of different BSSs, and the load of the system, the overall duration for passive scanning (scanning delay) may vary.

An example for passive scanning is depicted in Figure 2.16. On reception of the $\text{MLME-SCAN.request}$ from the SME with the parameters $\text{passive}$ and $\text{MaxChannelTime}$, the MLME initiates the scanning procedure. Further parameters are possible but have been omitted in this example. Since no particular channel list was requested, the terminal will subsequently scan each channel from the valid channel range for the appropriate PHY. Starting with channel 1, the terminal listens for beacon transmissions. The upper scanning duration thereby is limited by $\text{MaxChannelTime}$. After $\Delta_1$, the beacon is successfully received, which makes the terminal switching to the next channel and so forth. For channel 3, no
beacon detection is performed since the scanning duration exceeds MaxChannelTime. Obviously, beacon transmission does not take place at TBTT_2, but is delayed due to other transmissions. As a result, AP3 is not included in the MLME-SCAN.confirm message reported back to the SME after completion of the scanning procedure. This is how load in the network may distort passive scanning results. To cope with this problem, the SME needs to prescribe an increased value for MaxChannelTime. This, however, falls back to the resulting scanning delay as shown in Figure 2.16.

2.2.3.2 Active Scanning

Active scanning requires a station to generate specific request messages, so called *Probe frames*, with subsequent processing of incoming *Probe response* frames. Upon receipt of a MLME-SCAN.request with scan type ‘active’, a station shall use the following procedure for each channel to be scanned [67]:

a) Wait until the *ProbeDelay* time has expired or a PHYRxStart.indication has been received;

b) Perform the Basic Access procedure based on DCF;

c) Send a Probe with the broadcast destination, SSID, and broadcast BSSID;

d) Clear and start a ProbeTimer;

e) If PHYCCA.indication (busy) has not been detected before the ProbeTimer reaches MinChannelTime, then clear NAV and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses;

f) Clear NAV and scan the next channel.

The probe mechanism forces an AP to convey the same system information as done with the periodic beacon signal. In providing this information promptly on request, unnecessary waiting times of up to one entire Beacon Interval can be prevented. This is how active scanning shall support accelerated information provision, e.g., in the scope of supporting seamless handover. In addition, Probe response frames need to be acknowledged by stations to ensure integrity of data delivery. With passive scanning, ordinary beacons are sent as broadcast transmission so that a station might not receive full system information due to interference caused e.g., by hidden stations.
The previously describe active scanning procedure is illustrated in Figure 2.17. Note that other transmissions have not been taken up as for passive scanning. The SME triggers the active scanning procedure with a MLME-SCAN.request message. The terminal switches to Channel 1, waits a time span $\Delta_{\text{ProbeDelay}}$, performs DCF channel access (not shown) and broadcasts a Probe Request. Since a Probe Response is received within MinChannelTime, the terminal needs to further monitor the channel for the entire time span $\Delta_1 = \text{MaxChannelTime}$ prior to switching to Channel 2. Here, the same procedure takes place, but since there is no reply within $\Delta_2 = \text{MinChannelTime}$, the next channel is surveyed. The accumulative scanning delay for active scanning results from the respective interim scanning times $\Delta_{1-3}$, whereby these values always denote to either MinChannelTime or MaxChannelTime.

Impacts of scanning in WLAN systems according to IEEE 802.11 are investigated in Section 8.2.1. Both, active and passive scanning performance figures will be derived and benchmarked. It will be shown, that both approaches entail certain disadvantages that need to be overcome. The Hybrid Information System as essential part of this thesis offers respective means to improve the overall system performance in terms of accelerated system detection.
2.2.3.3 Scanning Summary

Each of the two scanning modes entails advantages and disadvantages. Accordingly, the Station Management Entity that chooses the respective scanning type needs to decide for the one or the other method.

Properties of passive scanning are:
+ No added traffic/load to the Radio Network;
+ Battery savings;
- Slow – each channel typically requires > 100 ms;
- Problems for delay-sensitive applications;
- Actual Beacon period depends on load in the system;
- Problems for non-synchronized systems and different Beacon period.

Properties of active scanning are:
+ Usually faster than passive scanning (40 - 300 ms due to [66]);
+ Data integrity due to acknowledged information provision;
- Probe requests/responses pollution → congestion if there are many scanning stations;
- Forces APs to send information being redundant to Beacons.

There are further factors that have an impact on the scanning performance, e.g., with respect to delay, making predictions difficult. For instance, scanning parameters MinChannelTime/MaxChannelTime as well as Beacon period can be chosen arbitrarily. In addition, system load affects both, active and passive scanning procedures: While active scanning will be delayed since probe requests cannot be sent while the channel is busy, passive scanning suffers from delayed beacon receptions. These problems further scale up with the number of different channels to be monitored.

A possible solution to speed up the scanning process is to restrict the number of scanning actions. The Hybrid Information Systems as proposed in Section 5 offers support in the way that self-conducted scanning is limited or becomes even obsolete. Even if a minimum of scanning activity is further required, the Hybrid Information System may be helpful in providing additional assistance data, e.g., knowing specific candidate channels supersedes the need for scanning the entire frequency band.
So far, the focus was put on scanning and synchronization aspects. The underlying reason hereby is to perform system detection. In order to allow for proper operation, additional information needs to be present to be acquired by specific measurements. The following section describes respective measurements as specified for IEEE 802.11.

### 2.2.4 Measurements in 802.11

Control of link adaptation, power control, and error correction schemes is highly dependent on detailed knowledge of up-to-date signal- and interference conditions in the field. Accordingly, all cellular systems specify the exchange of related information.

While many measurement parameters are defined for UMTS and GSM (see Table 2.4), legacy 802.11 offers only poor support. Recognizing the need for specific link information, a standard amendment for spectrum and transmit power management extensions, known as 802.11h [74], has been specified and was approved in 2003. Focus was put on two services: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). While 802.11h mainly addresses internal use of data, a further amendment is currently under preparation by IEEE 802.11 Task Group k, which will be referred to as 802.11k [75]. While 802.11h targets on spectrum management, 802.11k specifies further measuring options, which are referred to as radio resource measurements. A particular aim thereby is to allow for locally taken measurements on the one hand side as well as exchange of measurement information with peer stations including third parties and external sources on the other hand side. In this way, new services such as location-based services shall be encouraged.

Both amendments, 802.11h and k, introduce basic structures for requesting and reporting measurement information of 802 type only. No inter-RAT measurement procedures are defined and there is no standardized way of performing handover from WLAN to other cellular mobile radio networks. Interoperability between heterogeneous networks, however, is considered by the Media Independent Handoff Working Group IEEE 802.21 whose aim is to develop stan-

---

9 While 802.11h has already been approved, 802.11k is still subject to change. All information and figures compiled for this thesis refer to the latest available draft while writing, which is IEEE 802.11k/D2.0 from February 2005.
2.2. IEEE 802.11

... standards to enable handover and interoperability between heterogeneous network types including both 802 and non-802 networks [81].

A basic element of the Hybrid Information System as introduced in this work is to provide a means for measurement information transfer between heterogeneous systems. This mitigates the need for self-conducted intersystem measurements. Feeding of HIS thus is exclusively accomplished by intra-system measurements as specified e.g., by 802.11h and 802.11k. For this, the respective intra-system measurements as provided by these amendments are explained in more detail in the following.

2.2.4.1 Information Transfer

Stations may provide measurement information autonomously and/or on a regular basis. However, common practice is to generate respective reports as a response to previously received measurement requests. Legacy IEEE 802.11 defines three different MAC frame types: Management frames, Control frames and Data frames. Data frames are reserved for transporting layer 3 data, control frames handle the access to the medium and management frames serve for the administration of the Basic Service Set (BSS) and terminals. All spectrum management actions (802.11h) and radio resource management actions (802.11k) therefore use the management format.

The general MAC frame format is shown in Figure 2.18, Table 1. It comprises a set of fields that occur in a fixed order in all frame types. The first two octets serve as Frame Control to identify the type of frame to be transmitted. A subsequent two-octet Duration/ID field informs about the duration of each frame. Depending on the frame format, one to four Address fields are specified to announce sender and receiver of a particular message. The address field usage thereby is specified by the relative position of the address field within the MAC header. Furthermore, a Sequence Control field is present in some frame types, which is needed for de-/fragmentation and serialization of messages. A Frame Body field of variable length and a 32-bit Frame Check Sequence (FCS) field with a 32-bit Cyclic Redundancy Code (CRC) complete the general MAC frame format.

The initial Frame Control field provides a Type description field (data, control, or management) and a Subtype field for more specific information. Depending
on the chosen (sub-) type, the variable *Frame Body* field is assorted. For management frames of legacy 802.11, the subtype defines Association and Authentication fields, Probe directives, Beacons and Traffic Indication Announcements. To transmit spectrum management (802.11h) or radio measurement (802.11k) directives, a special management frame of subtype *Action* is used, which was newly defined within 802.11h, see Figure 2.18 Table 6.

### Figure 2.18: MAC frame formats in 802.11

A Management frame carrying an Action field in its Frame Body is shown in Figure 2.19 and Figure 2.20, Table 1 and Table 2. The Action field entry type *Category* (Table 3) specifies whether spectrum management or radio measure-
ment tasks are to be executed. Depending on the category, the corresponding Action field (Table 4) defines several actions to take place. Especially the ‘Measurement Request’ and ‘Measurement Report’ are of particular interest in this work and will be described in detail in Section 2.2.5 (802.11h) and 0 (802.11k). Other Action tasks as depicted in Table 4 of Figure 2.19 and Figure 2.20 will be addressed roughly only.

**Table 1: Management Frame Format (h+k)**

<table>
<thead>
<tr>
<th>Octets</th>
<th>Frame Control</th>
<th>Duration</th>
<th>DA</th>
<th>SA</th>
<th>BSSID</th>
<th>Sequence Control</th>
<th>FCS</th>
</tr>
</thead>
</table>

**Table 2: Action frame → Measurement Request Frame Body Format (h+k)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Action</th>
<th>Dialog Token</th>
<th>Number of Repetitions</th>
<th>Frame Restart Delay</th>
<th>Measurement Request Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectrum Management (h)</td>
<td>Measurement Request</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio Measurement (k)</td>
<td>Measurement Report</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measurement Request (h)</td>
<td>TPC Request</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measurement Request (k)</td>
<td>TPC Report</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3: Measurement Request Mode Field (h+k)**

<table>
<thead>
<tr>
<th>Bit</th>
<th>Enable</th>
<th>Request</th>
<th>Report</th>
<th>Duration Mandatory</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 2.19: Action Frame Format with Measurement Request**

The Action Frame → Measurement Report Frame Body Format (Figure 2.20, Table 2) is the same for 802.11h and k. The Measurement Request Frame Body Format (Figure 2.19, Table 2), however, has been slightly enhanced by 802.11k.
Two additional fields, *Number of Repetitions* and *Frame Restart Delay*, have been added. The first allows requesting for repeated execution of the indicated measurement while the second specifies the intermediate time span to be waited.

**Table 1: Management Frame Format (h+k)**

<table>
<thead>
<tr>
<th>Octets:</th>
<th>Frame Control (2)</th>
<th>Duration (2)</th>
<th>DA (6)</th>
<th>SA (6)</th>
<th>BSSID (6)</th>
<th>Sequence Control (2)</th>
<th>Frame Body (0 – 2312)</th>
<th>FCS (4)</th>
</tr>
</thead>
</table>

**Table 2: Action Frame Measurement Report Frame Body Format (h+k)**

<table>
<thead>
<tr>
<th>Measurement Report Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category (1)</td>
</tr>
</tbody>
</table>

**Table 3: Octets**

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectrum Management (h)</td>
<td>0</td>
</tr>
<tr>
<td>Reserved</td>
<td>1-4</td>
</tr>
<tr>
<td>Radio Measurement (k)</td>
<td>5</td>
</tr>
<tr>
<td>Reserved</td>
<td>6-127</td>
</tr>
<tr>
<td>Error</td>
<td>128-255</td>
</tr>
</tbody>
</table>

**Table 4: Action Name**

<table>
<thead>
<tr>
<th>Action Name</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Request</td>
<td>0</td>
</tr>
<tr>
<td>Measurement Report</td>
<td>1</td>
</tr>
<tr>
<td>TPC Request (h)</td>
<td>2</td>
</tr>
<tr>
<td>Link Measurement Report (k)</td>
<td>3</td>
</tr>
<tr>
<td>TPC Report (h)</td>
<td>4</td>
</tr>
<tr>
<td>Link Measurement Report (k)</td>
<td>5</td>
</tr>
<tr>
<td>Channel Switch Announcement (h)</td>
<td>6</td>
</tr>
<tr>
<td>Neighbor Report Request (k)</td>
<td>7</td>
</tr>
<tr>
<td>Neighbor Report Response (k)</td>
<td>8</td>
</tr>
<tr>
<td>Reserved</td>
<td>9-255</td>
</tr>
</tbody>
</table>

**Table 5: Measurement Report Element Format (h+k)**

<table>
<thead>
<tr>
<th>Element ID (1)</th>
<th>Length (1)</th>
<th>Measurement Token (1)</th>
<th>Measurement Report Mode (1)</th>
<th>Measurement Type (1)</th>
<th>Measurement Report (variable)</th>
</tr>
</thead>
</table>

**Table 6: Measurement Report Mode Field (h+k)**

<table>
<thead>
<tr>
<th>Bit</th>
<th>Late (0)</th>
<th>Incapable (1)</th>
<th>Refused (2)</th>
<th>Reserved (3-7)</th>
</tr>
</thead>
</table>

**Table 7: Measurement Type definition for Measurement Reports**

<table>
<thead>
<tr>
<th>Name</th>
<th>Measurement Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Report</td>
<td>0</td>
</tr>
<tr>
<td>Clear Channel Assessment (CCA) report</td>
<td>1</td>
</tr>
<tr>
<td>Receive Power Indication (RPI) Histogram Report</td>
<td>2</td>
</tr>
<tr>
<td>Channel Load Report</td>
<td>3</td>
</tr>
<tr>
<td>Noise Histogram Report</td>
<td>4</td>
</tr>
<tr>
<td>Beacon Report</td>
<td>5</td>
</tr>
<tr>
<td>Frame Report</td>
<td>6</td>
</tr>
<tr>
<td>Hidden Node Report</td>
<td>7</td>
</tr>
<tr>
<td>Medium Sensing Time Histogram Report</td>
<td>8</td>
</tr>
<tr>
<td>STA Statistics Report</td>
<td>9</td>
</tr>
<tr>
<td>LCI Report</td>
<td>10</td>
</tr>
<tr>
<td>Reserved</td>
<td>11-255</td>
</tr>
</tbody>
</table>

**Figure 2.20: Action Frame Format with Measurement Report**

Central elements of the Measurement Request frames and the Measurement Report frames are the Measurement Request Element and the Measurement Report Element, respectively (Tables 5). Both include a *Measurement Request/Report Mode* field (Tables 6) and a *Measurement Type* field (Tables 7). The *Measurement Request Mode* Field (Figure 2.19, Table 6) informs about the disposition of a station to accept autonomously sent requests or reports from other stations. An additional field as used by 802.11k allows specifying, whether the measurement
duration included in any request shall be considered as mandatory or aspired. The associated Measurement Report Mode Field (Figure 2.20, Table 6) gives feedback whether a respective measurement request was received in time or can (not) be replied. The Measurement Request/Report Type (Tables 7) fields are the actual information carriers. Depending on the type, specific measurement actions are performed by the receiving station. A detailed description of each of these Measurement Types is given in the following sections.

For the Action-type ‘Measurement’, a couple of Measurement Elements have been specified within 802.11h and 802.11k.

Spectrum Management for 802.11h defines measurement requests and reports of type
- Basic,
- Clear Channel Assessment (CCA), and
- Receive Power Indication Histogram.

Radio Resource Measurements for 802.11k supplement these measurement actions by requests and reports of type
- Channel load,
- Noise histogram,
- Beacon,
- Frame,
- Hidden Station,
- Medium sensing time histogram,
- STA statistics,
- Location Configuration Information (LCI), and
- Measurement Pause (request only).

Figure 2.21 depicts the information flow model adopted for spectrum management (802.11h) and radio measurement (802.11k). It is assumed that the initial decision for taking measurements is taken by the Station Management Entity (SME), which has been introduced in Section 2.2.3 and Figure 2.12. The SME generates a MLME-MREQUEST.req message, which is received by the MAC sublayer management entity (MLME) via the MLME-SAP (Service Access Point). The MLME is responsible for coordination of all actions of the
MAC layer. Being able to process the request, the MLME will acknowledge this with a **MLME-REQUEST.cfm** and trigger further actions. If the SME has requested self-conducted measurements, the MLME will run respective protocols for measuring. If the SME has requested measurements from another peer station, it will generate a *Measurement Request frame* as described earlier. Figure 2.21 depicts the case for requesting a peer station to perform measurements. As soon as the requested information is available, the MLME compiles a **MLME-MREPORT.ind** message to report gathered information to the SME.

---

**Figure 2.21: Information flow for measurements in 802.11h,k**

---

### 2.2.5 Specific Measurements in 802.11h

Spectrum management as introduced by 802.11h defines a couple of new *Information Elements* (= optional components or variable length fields transmitted in the frame body of *Management* frames, see Section 2.2.4.1). An overview of all IE of 802.11h together with a short explanation is given in Table 2.7.
### Table 2.7: Supported IEs for spectrum management in 802.11h

<table>
<thead>
<tr>
<th>Information Element (IE)</th>
<th>Element ID</th>
<th>Provided Information/Purpose</th>
<th>Used in subtype frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>17–31</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Power Constraint</td>
<td>32</td>
<td>Information on allowed max. local transmit power</td>
<td>Beacon frame Probe Response frame</td>
</tr>
<tr>
<td>Power Capability</td>
<td>33</td>
<td>Min. and max. power, with which a STA is capable to transmit</td>
<td>Association Request frame Reassociation Request frame</td>
</tr>
<tr>
<td>TPC Request</td>
<td>34</td>
<td>Request for a STA to report transmit power and link margin information</td>
<td>Action frame → TPC Request</td>
</tr>
<tr>
<td>TPC Report</td>
<td>35</td>
<td>Transmit Power (used for the frame) and link margin</td>
<td>With prior request: Action frame → TPC Report Without prior request: Beacon frame (no link margin) Probe Response (no link margin)</td>
</tr>
<tr>
<td>Supported Channels</td>
<td>36</td>
<td>List of channel subbands in which a STA is capable of operating</td>
<td>Association Request frame Reassociation Request frame</td>
</tr>
<tr>
<td>Channel Switch Announcement</td>
<td>37</td>
<td>Advertisement of a new channel the AP/STA switches to, a possible time span until switching and restrictions in between (if any)</td>
<td>Beacon frame Probe Response frame Action frame → Channel Switch Announcement</td>
</tr>
<tr>
<td>Measurement Request</td>
<td>38</td>
<td>Basic Request Clear Channel Assessment (CCA) Request Receive Power Indication (RPI) histogram Request</td>
<td>Action frame → Measurement Request</td>
</tr>
<tr>
<td>Quiet</td>
<td>40</td>
<td>Defines (periodic) intervals in which no transmission shall occur</td>
<td>Beacon frame Probe Response frame</td>
</tr>
<tr>
<td>IBSS DFS</td>
<td>41</td>
<td>Coordination of IBSS channel switch</td>
<td>Beacon frame Probe Response frame</td>
</tr>
</tbody>
</table>
The newly introduced information elements allow for exchange of capability information and commentatorship on specific link conditions. Important properties of the channel may be derived by applying these IEs: Reception strength of the TPC report that entails the transmit power with which it was conveyed allows for direct derivation of the pathloss. Application of the Quiet element may be used to assist in making channel measurements without interference from other STAs in the (I)BSS.

However, most important information elements in the scope of this thesis are the Measurement Requests/Reports shaded grey in Table 2.7. IEEE 802.11h Measurements Reports (MR) are generated autonomously or on request. The request may be sent to an individual (AP→STA or STA→AP) or group destination address (AP→STAs; STA→STAs for IBSS only), whereby the latter should be used with care to avoid reply storms [74]. Except for IBSS, STAs are not allowed to request other STAs for measurement reports. In general, all measurement requests and reports are enabled by default but an entity may announce that it will not accept any requests or autonomously sent reports, cp. Measurement Request Mode field in Figure 2.19 (Table 6 & Table 8). If enabled, a STA shall honor all other requests while an AP may ignore a request to disable a mandatory measurement request [74].

IEEE 802.11h measurement requests/reports always address one out of three types to specify further actions. The three types defined are Basic request/report, Clear Channel Assessment (CCA) request/report and Receive Power Indication (RPI) histogram request/report, see Table 7 in Figure 2.19, Figure 2.20. While support of Basic Report generation is mandatory for STAs, support for CCA reports and RPI histogram reports is optional.

The generic request field for either of these three measurement request types is shown in Figure 2.22. Transmission takes place in the Measurement Request field as shown in Table 5 of Figure 2.19. Parameters included in the request define the Channel Number, which specifies the channel to be scanned, a Measurement Start Time and the Measurement Duration. The latter has a length of 2 bytes reflecting a number of Time Units (TUs) that correspond to the designated measuring period T Measure. Accordingly, monitoring is performed for a time span of $1 \leq T_{\text{Measure}} \leq 2^{16}-1$ time units corresponding to $1024 \mu s \leq T_{\text{Measure}} \leq 67.12s$. As a rule of thumb, one can keep in mind that the upper bound for measurement durations in 802.11h and k comprises approximately one minute.
2.2.5.1 Basic Report

On reception of a measurement request of type *Basic Request*, a STA is obliged to perform required measurements and to reply with a *Basic Report*. The corresponding field format is shown in Figure 2.23. The initial three fields echo the channel number, the measurement start time and duration as included in a preceding request (if there was one). An additional field, the *Map* field, is added to convey measuring results. The Map field is coded as bit field with the following meaning:

<table>
<thead>
<tr>
<th>Bit</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>BSS:</strong> Indicates presence of other (I)BSS. A value of 1 denotes the reception of at least one valid <em>MAC Protocol Data Unit</em> (MPDU) during the measurement duration $T_{\text{Measure}}$.</td>
</tr>
<tr>
<td>1</td>
<td><strong>OFDM Preamble:</strong> Indicates presence of other OFDM based systems than 802.11a, e.g., HIPERLAN/2. A value of 1 denotes the reception of at least one sequence of short training symbols without subsequent valid Signal field.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Undefined Signal:</strong> Detection of significant power that cannot be characterized as valid MPDU, OFDM preamble or radar.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Radar:</strong> Detection of radar operating in the channel during the measurement duration</td>
</tr>
<tr>
<td>4</td>
<td><strong>Unmeasured:</strong> Indicates whether requested channel was measured (1) or nor (0).</td>
</tr>
<tr>
<td>5-7</td>
<td><strong>Reserved:</strong> -</td>
</tr>
</tbody>
</table>
2. System Overview

2.2.5.2 Clear Channel Assessment (CCA) Report

On reception of a measurement request of type *CCA Request*, a STA optionally generates a corresponding CCA Report as reply. The corresponding field format is shown in Figure 2.24. The initial three fields echo the channel number, the measurement start time and duration as included in a preceding request (if there was one). An additional field, the *CCA Busy Fraction* field, is added to convey measuring results.

![Figure 2.24: Measurement Report field of type CCA report](image)

To compile a CCA report the terminal surveys the channel status applying a resolution on the time scale of microseconds. The fractional duration over which the CCA indicated the channel was busy during the measurement duration is calculated hereafter by equation (2.5):

\[
CCA _ { Busy _ Fraction } = \text{Ceiling} \left[ \frac{255 \times \text{Duration CCA indicated channel was busy (\mu s)}}{1024 \times \text{Measurement duration (TUs)}} \right]
\]  

(2.5)

2.2.5.3 Receive Power Indication (RPI) Histogram Report

On reception of a measurement request of type *RPI Histogram Request*, a STA optionally generates a corresponding RPI Histogram Report as reply. The corresponding field format is shown in Figure 2.25. The initial three fields echo the
Channel number, the measurement start time and duration as included in a preceding request (if there was one). The actual outcome of the measurement is conveyed as RPI histogram. Each of the RPI levels thereby is coded with an eight-bit field.

**Figure 2.25: Measurement Report field of type RPI histogram report**

Determination of the fractional part of each RPI level is likewise to the approach for CCA Busy Fraction. The received power level on the specified channel is recorded during the entire measurement duration and a classification in one of the 8 RPI levels according to Table 2.8 is performed.

**Table 2.8: RPI levels as defined within 802.11h**

<table>
<thead>
<tr>
<th>RPI Level</th>
<th>Power observed at Antenna (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>[−∞, −87]</td>
</tr>
<tr>
<td>1</td>
<td>[−87, −82]</td>
</tr>
<tr>
<td>2</td>
<td>[−82, −77]</td>
</tr>
<tr>
<td>3</td>
<td>[−77, −72]</td>
</tr>
<tr>
<td>4</td>
<td>[−72, −67]</td>
</tr>
<tr>
<td>5</td>
<td>[−67, −62]</td>
</tr>
<tr>
<td>6</td>
<td>[−62, −57]</td>
</tr>
<tr>
<td>7</td>
<td>[−57, +∞]</td>
</tr>
</tbody>
</table>
In the end, the fraction of time with which each RPI level was received is calculated by equation (2.6) and the result is written to the respective density field of Figure 2.25.

\[
\text{RPI}_X \_ \text{density} = \text{Ceiling} \left[ \frac{255 \times \text{Duration receiving at RPI value (\mu s)}}{1024 \times \text{Measurement duration (TUs)}} \right].
\] (2.6)

The sum of the densities at the receiving end will be approximately 255, but can end up to 262 due to rounding effects. The density resolution of each single field is limited by a number of 8 bits used for transmission. Hence, data integrity is bounded to 1/256, which means a maximum deviation of 0.4 % has to be accepted.
CHAPTER 3

Integration & Cooperation of Radio Access Networks

Content

3.1 Introduction .........................................................................................57
3.2 State of the Art Overview ....................................................................59
3.3 Mobility & Handover ..........................................................................76
3.4 Trigger .................................................................................................94

Keywords: System Integration, Mobility, Inter-system Handover, Decision Criteria

The following chapter deals with different aspects of system integration. First, an overview of related research is given. Standardization bodies, fora, and international research projects consider cooperation of heterogeneous networks. A comparison of different integration efforts works out their foci and commonalities. Hereafter, general aspects of mobility are presented. Particularly, terminal mobility is addressed resulting in the necessity to support handover. Different origins for handover triggering will be presented, whereby particular properties of the vertical handover as addressed in this thesis will be put into focus.

3.1 Introduction

It is widely recognized that next generation wireless systems will need to feature by incorporative aspects. The reasons for this are manifold: First, the perception, that dedicated systems are more suitable to provide specific services to the user, will result in complementary system design. Even today, different systems for ultra short-range, short-distance and wide area communication exist. This leads to specific deployments of Personal Body Networks, Wireless Local Area Networks, and Cellular Networks.
Figure 3.1: Development towards 4G

Second, cooperation of systems in the same or adjacent spectrum will further increase. Due to spectrum scarceness, de-regulation efforts for increased market competition and political reasons, the number of systems operating in direct impact sphere of each other will further increase. To allow for proper incorporation, ‘live and let live’ doctrines are necessary. Research in this field includes listen before talk approaches, frequency-sharing rules [17] for dynamic and static sharing and game theoretical approaches [86].

Third, the migration from current 2.5/3G systems to systems beyond 3G will proceed stepwise. This means, that future systems need to entail a certain degree of backwards compatibility. Coexistence with antecessor generations thus is an existential requirement. This is also indicated in Figure 3.1: Though next generation mobile networks pave their way, coexistence with previous generations will require cooperation. Multiband terminals with adaptation capabilities will serve as enablers for complementary network usage. An important key word in this context is also Software Defined Radio (SDR) that supports the integration process by easy redefinition of mobile functions and protocols [87][88][89].

For all the above-given reasons, system cooperation and -integration is of fundamental interest. This is also expressed by ongoing research. Comprehensive international IST projects in the context of the 6\textsuperscript{xt} European Framework Programme (FP6) such as Ambient Networks [39] or WINNER [41] define respective research tasks.
3.2. State of the Art Overview

Though systems generally are conceptualized in a complementary manner, this does not mean that there are no overlapping domains. The term ‘overlapping’ thereby addresses different areas, in particular coverage (space domain) and QoS support (service domain). As such, overlapping network properties are the elementary foundation based on which the target of Always Best Connected becomes feasible.

3.2 State of the Art Overview

The following subsections reflect the importance of system cooperation by presenting a comprehensive overview of related fora and research projects with respect to mutual system support. The description\(^\text{10}\) contains recently concluded projects, ongoing research, and upcoming activities being just in an initial state of their producing. All these activities emphasize the worldwide seen necessity for further research in the field of system cooperation.

3.2.1 Standardization Bodies & Fora

Reflecting ongoing work with respect to system integration points up the enormous interest as seen by the research community. While some projects target on a high-level overall solution, others focus on particular aspects. In the following, a short overview of system and service integration tasks will be given showing major trends as seen by dedicated consortia. An encompassing description along with detailed answers to the above questions is provided within ANWIRE D1.5.1 ‘Integrated System and Service Architecture’ [18].

3.2.1.1 ETSI BRAN/3GPP

In its first technical report on ‘Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular Systems’ [19], two approaches, loose coupling and tight coupling, were taken by ETSI BRAN. The objective is system integration between HIPERLAN/2 (H/2) and UMTS, depending on the requirements and the feasibility of deployment. Figure 3.2 exemplarily depicts different levels of WLAN coupling with UMTS.

\(^{10}\) Parts of this section derive from active collaboration of the author within related fora and projects, e.g., BRAIN, MIND, ANWIRE and VDE-ITG 5.2.4 and WINNER.
The *loose* coupling approach is simple to implement without major modifications to the systems. It allows centralized authentication and signaling information related to a user, independent of the radio access network. However, it does not allow for seamless handover between the systems since the local IP address needs to be changed and the QoS for each connection has to be renegotiated.

The *tight* approach, on the other hand, allows for seamless interworking, reusing the mechanisms for mobility, QoS, and security of the UMTS core network for H/2. Furthermore, certain addresses and identifiers of UMTS are used by H/2. However, this increases the system complexity and signaling. The standardization work carried out in ETSI BRAN/3GPP provides a good overview of the variety of approaches that can be adopted, but several aspects in mobility and handover are still open.

Based on the results of [19], ETSI BRAN originally had started further work on a Technical Specification TS 101 961, to specify the architectures and protocols of a HIPERLAN/2 network that interworks with 3G networks. However, work on this item has been stopped in 2003.

Similar to the ETSI BRAN standardizations efforts and to a certain extent based on it, 3GPP in TSG SA1 (Services) considers coupling for WLAN/3GPP interworking. Rather than distinguishing only between loose and tight coupling, 3GPP considers different levels of interworking in its technical report ‘Feasibility Study on UMTS-WLAN interworking’ [22]. In addition, the considered WLAN technology is no longer restricted to HIPERLAN/2. IEEE 802.11a,b as well as Bluetooth have been added as candidate WLAN technologies.

The study covers service use cases in the scenarios as well as the impact on the specification on the standard that will be required for the inclusion of the specific type of coupling and level of interworking. The investigated scenarios con-
3.2. State of the Art Overview

consider systematic increase of network integration, ranging from simple 3G-WLAN interworking using common billing & customer care to seamless inter-system operation i.e., allowing access to services provided by entities of the 3GPP Circuit Switched (CS) Core Network over WLAN.

The six scenarios that were investigated comprise:

- **Common Billing and Customer Care:** This scenario is the simplest interworking scheme with association between systems by a common customer relationship i.e., single bill from the mobile operator and an integrated customer care.

- **3GPP System based Access Control and Charging:** Here, authentication, authorization, and accounting are provided by the 3GPP system. The security level of these functions applied to WLAN is in line with that of the 3GPP system, providing the means for the operator to charge access in a consistent manner over both platforms.

- **Access to 3GPP System packet switched based Services:** This is to allow the operator to extend 3GPP system packet switched services to the WLAN, allowing services such as location based services, SMS, MMS, etc.

- **Service Continuity:** This scenario allows services to be maintained after vertical handover between WLAN and a 3G system. Here, any change of access may be noticeable to the user.

- **Seamless Services:** This scenario provides seamless service continuity minimizing data loss and break time during the handover.

- **Access to 3GPP System circuit switched based Services:** This scenario allows access for access to services provided by the entities of the 3GPP Circuit Switched Core Network over WLAN, providing seamless and user-transparent handover.

These scenarios provide a path for evolution from entry-level services (loose coupling) to full availability of 3GPP services (very tight coupling) to the WLAN access user. With a stepwise increasing level of service, a deployment initially directed at one service scenario provides the basis for further development. Main characteristics and capabilities of each scenario are summarized by Table 3.1.
Due to increased interworking requirements, further specifications were brought on the way within 3GPP. Requirements on 3GPP system to WLAN interworking have been specified in [23]. A ‘System description’ and a ‘Functional and architectural definition’ are provided in [24] and [25], respectively. Additional important aspects such as telecommunication and charging management [26] as well as interworking security aspects [27] complement the 3GPP-WLAN system integration framework.

Handover capabilities for combinational services between WCDMA and WLAN networks are currently being considered for inclusion in 3GPP Release 8. The Hybrid Information System as proposed in this work provides an important contribution towards this development.

Table 3.1: WLAN/3G Interworking Scenarios defined within 3GPP [22]

<table>
<thead>
<tr>
<th>Scenarios: Service &amp; operational Capabilities:</th>
<th>loose</th>
<th>loose</th>
<th>loose</th>
<th>tight</th>
<th>very tight</th>
<th>very tight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scen. 1: Common Billing &amp; Customer Care</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scen. 2: 3GPP System based Access Control &amp; Charging</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scen. 3: Access to 3GPP System PS based Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scen. 4: Service Continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Scen. 5: Seamless Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Scen. 6: Access to 3GPP System CS based Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Common billing X X X X X X
Common customer care X X X X X X
3GPP system based Access Control
X X X X X X
Access to 3GPP system PS based services from WLAN
X X X
Service Continuity X X
Seamless Service Continuity X
Access to 3GPP system CS based Services with seamless mobility X
3.2.1.2 IEEE

IEEE addresses different standardization activities, each dealing with a specific topic. While in the beginning only aspects of homogeneous system management have been addressed, a couple of new groups have been founded in the last 2-3 years coping with interoperability and integration aspects. The most important ones will be shortly presented in the following.

3.2.1.2.1 IEEE 802.11u: Interworking with External Networks

IEEE 802.11u formerly was known as *Wireless Interworking with External Networks* (WIEN) Study Group. Approval as full task group was given in December 2004. By providing amendments to the IEEE 802.11 PHY/MAC layers, interworking with other (external) networks shall be enabled. Similar to external bodies such as 3GPP that define interworking capabilities from the cellular perspective, IEEE 802.11u shall specify logical counterparts from 802.11 point’s of view, which can only be addressed within the IEEE 802.11 project. This shall allow external networks to interwork with IEEE 802.11 equipment in a common, harmonized, and standardized manner. Two main areas thereby will be addressed: Enhanced protocol exchanges across the air interface and definition of primitives to support interaction with higher layers. This includes specific interfaces to support external authentication, authorization, and accounting, together with network selection, encryption, policy enforcement, and resource management. In addition, interfaces to existing IEEE 802.11 functions, e.g., 802.11i, shall be considered.

There is another project within IEEE 802 with similar scope as 802.11u, referred to as IEEE 802.21, which will be shortly introduced in the next section. In order to avoid overlapping in the scopes of the two projects, an agreement for ongoing formal coordination has been made between IEEE 802.21 and IEEE 802.11 WIEN SG, the predecessor of IEEE 802.11u.

3.2.1.2.2 802.21 Media Independent Handoff Working Group

IEEE 802.21’s aim is to develop standards to enable handover and interoperability between heterogeneous network types including both 802 and non-802 networks. After meeting as an *Executive Committee Study Group* (ECSG) for one year, 802.21 has been approved by IEEE as a full IEEE WG in February 2004 [28].

A key role within 802.21 is played by the so-called *Link Layer Triggers* (L2 triggers) [29], cp. Section 3.4, since their availability and evaluation is essential
for handover optimization. Furthermore, general handover information definition and transport is addressed by 802.21, which also incorporates cellular coupling methods. Accordingly, the *Project Authorization* (PAR) at IEEE was given for ‘Media Independent Handover Services’. Future tasks of this working group include definition of useful L2 network detection mechanisms. For this, a close cooperation with the IETF *Detecting Network Attachment* (DNA) working group and the IRTF MobOpts working group is aimed at. Further (in)formal liaisons efforts with IEEE 802.16 as well as 802.11r/WNM /WIEN.u are on the way.

Since 802.21 considers handoffs between *all* IEEE 802 wireless technologies and cellular networks, the task of 802.11 interworking with cellular networks being actually a focus of 802.11u seems to be covered twice. However, the 802.11u PAR [30] gives the following reasons for which the two projects differ: First, IEEE 802.21 will not be able to amend IEEE 802.11. Instead, existing IEEE 802.11 amendments will be considered to enable interworking. Second, while IEEE 802.21 considers terminals with multiple air interfaces, IEEE 802.11u only considers aspects, which affect the IEEE 802.11 air interface.

### 3.2.1.3 IETF

Contrary to the previously discussed IEEE working groups, the focus of the *Internet Engineering Task Force* (IETF) in the context of system integration is on L3 connectivity and above. According to the ISO/OSI model, radio connectivity is subject to L2 while L3 should be decoupled from any radio specific impacts. However, signal propagation with fading effects does have significant impact on higher layer protocols as known from e.g., TCP over wireless [31]. This is why dedicated working groups within IETF have taken up the topic of link layer triggers (L2 triggers) to be used by higher layer protocols. L2 triggers are an important subject in the context of this thesis, since they are used in the decision making process for handover execution controlled by the Hybrid Information System. Hence, L2 triggers and related research will be described separately in Section 3.4.

It is worth mentioning that system integration is a goal whose accomplishment necessitates support by all layers. Since this thesis concentrates on radio aspects, higher layer integration aspects and core network activities as mainly addressed by IETF will be described only roughly for the sake of completeness.
The purpose of the *IETF Detecting Network Attachment* (DNA) Working Group [32] is to define standards that allow hosts to detect their IP layer configuration and connectivity status quickly and would allow a host to reconfigure its IPv6 layer faster than today. Indications currently available from a subset of wireless link layer technologies thereby may be exploited.

System Integration in the sense of macro mobility support across (radio) network boundaries is the scope of the *IETF Working Groups Mobility for IPv4* (mip4) [33] and *Mobility for IPv6* (mip6) [34], respectively. IP mobility support, better known as *Mobile IP*, allows a node to continue using its permanent home address as it moves. The Mobile IP protocols support transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. Therefore, the Mobile IP procedure is also referred to as L3 handover, see Section 3.3.2.6. In addition to the basic Mobile IP specifications, a whole family of complementary IETF drafts has been generated covering related topics such as deployment, routing optimization, security, and AAA.

### 3.2.1.4 ITU-T

Within the *Telecommunication Standardization Sector of the International Telecommunication Union* (ITU-T), standardization work is carried out by ITU-T Study Groups. The *Study Group 13 ‘Next Generation Networks’* [35] is responsible for studies relating to the architecture, evolution, and convergence of future generation networks. Amongst others, this includes frameworks and functional architectures, signaling requirements and interoperability. Convergence as addressed by the study group implies architecture and service convergence, interoperability between fixed and mobile networks as well as integration of satellite with terrestrial and Next Generation Networks (NGNs).

### 3.2.1.5 WWRF

The *Wireless World Research Forum* (WWRF) [36] is a global organization, which brings together experts from different domains such as manufacturers, network operators/service providers, R&D centers, universities as well as small and medium enterprises. Being founded in August 2001, WWRF addresses research tasks being relevant to future mobile and wireless communications, including pre-regulatory impact assessments. Accordingly, WWRF tends to cooperate closely with other fora and standardization bodies such as the UMTS Forum, ETSI, 3GPP, IETF, ITU, and other relevant panels.
Main objectives are formulation of strategic visions on future research directions in the mobile and wireless area; generation, identification and promotion of technical trends for mobile and wireless systems technologies; and enabling of global R&D collaboration. A common vision of future mobile and wireless technologies has been published in the ‘Book of Visions’ [37][38].

Current research topics with respect to system integration comprise amongst others system concepts and high-level architectures, requirements on future mobile and wireless systems, cooperative and ambient networks, inter-cell coordination and reconfiguration aspects.

Research on dedicated topics is undertaken by respective Working Groups and Special Interest Groups. Working Group 3 deals with ‘Co-operative and Ad-Hoc Networks’. The aim of the sub-working group Co-operating Networks is to define a framework architecture and related components. This includes ambient networks technologies and network technologies to support cognitive networks and radios. In addition, protocols, architectures, reference models, and transversal network aspects fall in this domain.

3.2.2 Research Projects

In addition to previously presented standardization bodies and fora, different research projects have taken up the challenging topic of system integration. The following section provides a non-exhaustive overview of respective research initiatives in alphabetical order.

3.2.2.1 AMBIENT NETWORKS

Ambient Networks (AN) is an Integrated Project (IP), co-sponsored by the European Commission under the Information Society Technology (IST) priority of the 6th Framework Programme (FP6). The project addresses the strategic objective of mobile and wireless systems beyond 3G. Together with three partner IPs, Wireless World Initiative New Radio (WINNER), End-to-End Reconfigurability (E²R) and MobiLife, it is part of the Wireless World Initiative (WWI) framework.

System integration is a substantial part of a new vision due to Ambient Networks in order to allow for dynamic composition of networks. The aim is to provide access to any network, including mobile personal networks, through instant es-
establishment of inter-network agreements. The underlying design paradigm is based on horizontally structured mobile systems that offer common control functions to a wide range of different applications and air interface technologies. Such a radical change requires the definition of new interfaces and a multitude of standards in key areas of future media- and context-aware, multi-domain mobile networks [39].

At the end of the project, a coherent wireless network solution is aimed at including an architecture proposal for self-configuring network components to reduce deployment and operational costs. In addition, an encompassing protocol suite for network composition evolved from IPv6 shall be covered by the project’s results.

### 3.2.2.2 ANWIRE

The *Academic Network for Wireless Internet Research in Europe* (ANWIRE) is a thematic network funded in the 5th Framework Programme of the European Commission. Scope of ANWIRE was the integration of today’s and future mobile systems with special focus on wireless Internet and reconfigurability [52]. Work was split up into task forces.

The ‘System Integration’ task force of ANWIRE had the goal to organize and coordinate activities on mechanisms that allow the integration of different systems. Thus, attention was focused on incorporating and integrating results of closely related fields like ‘Efficient and always on connectivity’, ‘Application architectures for the support of Reconfigurability and Adaptability’ or ‘Adaptable Service Architectures’ [53].

Starting with a detailed review of related system integration projects, requirements on interworking were derived [54] including non-technical aspects such as business models [55]. Major achievement was the definition of a 4G *Generic ANWIRE System and Service Integration Architecture* (GAIA) to cope with challenges of integrated future wireless networking. Policy-based network management [56][57] is considered as one main method to achieve the ABC target.

### 3.2.2.3 BRAIN/MIND

The projects *Broadband Radio Access for IP based Networks* (BRAIN) [45] and *Mobile IP based Network Developments* (MIND) [46] had the overall aim to provide customized broadband multimedia services to mobile users from a wide range of wireless access technologies such as GPRS/UMTS, WLAN (mainly based on H/2), personal area- and ad hoc networks. The BRAIN/MIND projects
designed a flexible and open framework allowing the use of any kind of mobility management protocol, QoS, AAA, and security solutions inside each access network based on ongoing efforts at the IP level in the IETF. The projects had developed their own scalable and robust micro-mobility protocol, mechanisms for end-to-end QoS support over heterogeneous networks, seamless horizontal/vertical handovers, and adaptation of multimedia services to the terminal and network conditions. An overview of integration of next generation mobile systems and wireless IP networks covering the MIND approach is given in [58]. Specific results related to interworking of WLAN and 3G have been published in [59].

3.2.2.4 DRIVE/OverDRIVE
The overall objective of the Dynamic Radio for IP-Services in Vehicular Environments (DRiVE) project and its follow-up Spectrum Efficient Uni- and Multicast Services over Dynamic Multi-Radio Networks in Vehicular Environments (OverDRIVE) have been to enable spectrum-efficient, high-quality wireless IP in a heterogeneous, multi-radio environment. This should enable the delivery of in-vehicle multimedia services, which ensure universally available access to information and support for education and entertainment. To achieve this objective, the projects addressed the convergence of cellular and broadcast networks to lay the foundation for innovative IP-based multimedia services. For this, DRiVE tackled two key aspects: First, interworking of different radio systems (GSM, GPRS, UMTS, DAB, DVB-T) in a common frequency range with dynamic spectrum allocation. Second, cooperation between network elements and applications in an adaptive manner. Furthermore, DRiVE designed location dependent services that adapt to the varying conditions of the underlying multi-radio environment. The DRiVE network architecture consists of a backbone, which connects the various available access systems, and the DRiVE functions, which are provided in both, backbone and access systems. The user is able to communicate with corresponding nodes through multiple access systems simultaneously. Additional aspects addressed by OverDRIVE comprise efficient Mobile Multicast (MMC) techniques as well as mechanisms for spectrum sharing between systems using Dynamic Spectrum Allocation (DSA) according to the actual load.
3.2.2.5 FLOWS

Similar to the previous projects, the Flexible Convergence of Wireless Standards and Services (FLOWS) [50] project used a common access network based on IP. Based on this, a variety of wireless access points is deployed using GSM, UMTS, or H/2. The project attempted to ensure that the impact of using multiple standards takes into account the business needs of users. Additional key target was to exploit the flexibility offered by Multiple Input/Multiple Output (MIMO) techniques to achieve convergence of wireless standards.

3.2.2.6 FuTURE

Future Technology for Universal Radio Environment (FuTURE) [51] is a key project in the wireless communication branch of the National High Technology Research and Development Program of China (863 Program). The technology objective of FuTURE is to carry out investigations on key technologies for air interface of Beyond 3G mobile communication, Beyond 3G radio access techniques; WLAN and ad hoc; MIMO and RF; also key topics as IPv6-based mobile core network.

The FuTURE project focuses on physical layer aspects of future wireless systems, providing a spectrum distribution for universal radio environment and an integrated architecture of a future wireless system. Some new network concepts, sub-system structures, handover methods, and access schemes have been proposed. For instance, a new multiple access scheme LAS-CDMA (Large Area Synchronized CDMA) has been accepted by 3GPP2 as one candidate for B3G standard. It is compatible with future all-IP networks and current wireless communication standards.

3.2.2.7 MOBIVAS

The Mobile Value-Added Services (MOBIVAS) [49] project developed a middleware platform for flexible delivery of value-added services over disparate reconfigurable network infrastructures. A loose coupling approach is adopted, with the middleware platform residing in the IP backbone, outside a particular access network (e.g., GPRS, UMTS). VAS are automatically deployed on multiple networks, based on intelligent interpretation of service and network profiles, and identification and actuation of appropriate reconfiguration actions. Independently of which operator provides them with connectivity, mobile users are offered personalized, context-aware discovery and delivery of downloadable application from a single portal, which acts as a one-stop-shop. Terminal-,
and network profile management are important enablers for these tasks. Moreover, charging, billing and accounting are handled in a unified manner.

3.2.2.8 STRIKE

*Spectrally Efficient Fixed Wireless Network based on Dual Standards* (STRIKE) aimed at proposing a spectrally efficient wireless broadband access by using interworking between heterogeneous wireless broadband networks. System integration is of particular interest to ensure both, an end-to-end QoS and the in-house and out-house coverage. Special attention hereby is put on the cooperation of existing WMAN and WLAN standards. HIPERMAN (WMAN) provides coverage in the outside area and HIPERLAN/2, respectively IEEE 802.11, (WLAN) cover the indoor area. A spectral efficiency enhancement is proposed in the STRIKE project using multiple antenna techniques.

3.2.2.9 SUITED

The framework of *Multi-Segment System for Broadband Ubiquitous Access to Internet Services and Demonstrator* (SUITED) [44] consisted of an integrated system, the *Global Mobile Broadband System* (GMBS). This is an IP-based mobile network comprising both, satellite and terrestrial (UMTS, GPRS, WLAN) components. A prototype of the GMBS was tested consisting of a multi-segment infrastructure and a multi-mode mobile terminal, capable of operating seamlessly with satellite and terrestrial networks. Navigation capabilities were integrated into the user terminal in order to enhance the performance of personal communication services.

3.2.2.10 TRUST/SCOUT

The main topic of the *Transparency Re-configurable Ubiquitous Terminal* (TRUST) [47] and *Smart User-centric Communication environment* (SCOUT) [48] projects was the use of reconfigurability in wireless access networks providing a high level of integration (by very tight coupling). This approach provides seamless interworking, better radio network planning and design, improved QoS and mobility support. The major drawbacks in this method are higher levels of signaling between the entities as well as requirement for definitions of suitable interfaces.
3.2.2.11 WINE GLASS

The objective of *Wireless IP NEtwork as a Generic platform for Location Aware Service Support* (WINE GLASS) [40] was to exploit enhanced IP-based techniques to support mobility and soft-guaranteed QoS in a wireless IPv6 Internet architecture incorporating UMTS and WLAN, and to explore their potential in enabling location- and QoS-aware application services for wireless mobile users. From QoS point of view DiffServ architecture has been chosen to provide QoS in the IP backbone where no Connection Admission Control is performed; availability of resources is guaranteed by an over-provisioning of the capacity. On the other hand, *Connection Admission Control* (CAC) is performed in the UTRAN access thanks to the AAA attendant function on the UTRAN-IP Gateway. In the WLAN access network, no QoS is provided since this is not supported by 802.11b technology.

From service point of view, the project provides a location aware service platform. This platform enables the applications to take full advantage of the location of the mobile node and evaluate the support of mobility and soft-guaranteed QoS in the underlying wireless Internet architecture.

From mobility point of view, Mobile IPv6 is used for macro mobility between access networks of the same or different technology. The project focuses more on macro mobility than micro mobility.

3.2.2.12 WINNER

Similar to Ambient Networks, *Wireless World Initiative New Radio* (WINNER) is an integrated IST project covered by FP6. The key objective is to develop an entirely new radio interface that allows for ubiquitous broadband radio access. One single radio system shall cover all scenarios from short range to wide area.

Work within WINNER is split up into Work Packages (WPs), from which WP4 explicitly addresses ‘Cooperation of Radio Access Systems’. Cooperation between different RANs is investigated regarding vertical handover, AAA, and *Common Radio Resource Management* (CRRM).

Since cooperation was not a primary requirement in the design of existing RANs, application of existing schemes is limited to higher layers only. The main innovation of WINNER hence will be to propose and develop respective schemes at the radio segment level. Due to [41], they will become built-in features of the WINNER interfaces.
3.2.3 Comparison of Integration Efforts

The previous state-of-the-art description pointed up the enormous efforts with respect to system integration activities. The following section provides a classification of integration efforts. Applied criteria comprise the types of network access technologies to be integrated (Figure 3.3), the achieved integration level at the management and control planes (Figure 3.4), the coupling levels of QoS and mobility (Figure 3.5a), the achieved vertical handover (Figure 3.5b) and the efforts related to adaptability and reconfigurability (Figure 3.6). Results as presented in the following are based on active contributions of the author in the framework of the ANWIRE project. For a detailed discussion of the results, please refer to [42].

3.2.3.1 Access technologies integration efforts

Regarding the types of access networks integrated in the framework of the reviewed projects, despite SUITED that also incorporates satellite-based communications, most of the projects care about the integration of terrestrial access networks, see Figure 3.3. The integration of Ad Hoc networks is an emerging topic of investigation considered mainly in the projects MIND, FuTURE and ANWIRE.

![Figure 3.3: Projects technologies integration effort](image)

1: UMTS & HIPERLAN/2 integration  
- ETSI BRAN/3GPP  
2: UMTS & WLAN integration  
- WINE GLASS  
3: UMTS & GPRS & WLAN & Satellite  
- SUITED  
4: Heterogeneous access networks  
- Moby Dick  
- BRAIN  
- DRIVE, OverDRIVE  
- TRUST/SCOUT  
- MOBIVAS  
- WWRF  
- FLOWS  
5: Heterogeneous and Ad hoc networks  
- MIND  
- FuTURE  
- ANWIRE

---

11 Considering radio access, WINNER puts the focus on definition of an entirely new air interface being the reason why it is not included in the figure.
3.2.3.2 Control and Management Integration

Other differences and commonalities were found for the integration efforts in the control and management planes of each project (see Figure 3.4). For instance, in BRAIN/MIND and WINE GLASS, the (Vertical) Handover process was achieved at a higher layer, i.e., session or network based, which herein is considered as a low integration method for HO. In contrast to this, HO managed at link or physical layer as aspired by e.g., TRUST/SCOUT is considered as a highly integrated mechanism. Due to loose and tight coupling-schemes, ETSI BRAN addresses both mechanisms for which the proposal is classified as both, low and high HO integration scheme.

Concerning Quality of Service (QoS) support over heterogeneous networks, some approaches such as FuTURE, ETSI BRAN, SUITED, BRAIN/MIND, WINE GLASS, and MOBIVAS use a low integration strategy applying QoS mapping. Others, such as Moby Dick, use a higher integration approach by specifying a common set of QoS classes.

![Figure 3.4: Control and management integration in heterogeneous technologies](image-url)
As for Authentication, Authorization and Accounting, projects like BRAIN/MIND and MOBIVAS apply different AAA concepts in each access network. Integration is given by means of exchanging database information (low AAA integration). High integration was achieved by ETSI BRAN, WINE GLASS, and Moby Dick that define commonly used AAA databases and protocols.

Furthermore, the high integration of radio access technologies at link or physical layer marks the differences with respect to the achieved level of System technology integration among the projects; other alternatives such as FuTURE, FLOWS, ETSI BRAN and SUITED use the required signaling between different radio access technologies for the exchange of information.

Finally, the Terminal architecture at lower layers differentiates the different projects into two groups; those that include multimode terminals using different interfaces for each radio access technology (low integration), and others that define multimode terminals using the same interface for different radio access technologies (high integration).

3.2.3.3 Mobility and Handover Integration
Seamless horizontal handover was an important aspect of mobility management considered in most of the integration projects. The seamless HO provides both, fast and smooth handover. Only, the FuTURE project introduces a mechanism for smooth handover in its framework, which mainly reduces the loss of packets being a precondition for minimization of delay. Significant importance in this area has the achieved level of coupling of QoS- and Mobility Management leading to different ways of reducing the delay in the re-establishment of QoS support after an HO event. Tighter coupling being necessary for seamless HO and faster QoS re-establishment, is achieved using mobility management signals to trigger QoS mechanisms. Figure 3.5a illustrates the horizontal HO approaches used in different projects.
Figure 3.5: Technology integration level and handover classifications

Figure 3.5b gathers the projects in terms of their efforts in the achieved vertical HO. (Other kinds of mobility between different technologies such as session-based mobility (SIP-Proxy) are not represented in the figure). The Policy Based Handover has raised special attraction in recent projects, where the mobile nodes can handoff from one technology to another based on other constraints (e.g., user-related such as service costs and performance, or network-related such as load balancing or QoS requirements) than the sole radio conditions being mainly the reason for ‘classical’ HO execution.

3.2.3.4 Adaptability and Reconfigurability Integration

Finally yet importantly, Figure 3.6 groups the projects with respect to their efforts in adaptability and reconfigurability. Within ANWIRE, adaptability was defined as the ability of communication nodes to change dynamically between predefined states. Reconfigurability, however, is the capability of communication nodes to change dynamically from one state to a new one that was not reachable or existing before. The transition thereby relies on prior external interactions.
3.3 Mobility & Handover

Mobile radio systems cover two basic human needs: Communication and Mobility. At first glance, both actions seem to be well defined; however, inherent manifestations are manifold.

Communication addresses any kind of information exchange including circuit/packet switching, unicast/multicast/broadcast and man/man, man/machine, machine/machine dialog. Similar diverse manifestations apply with respect to mobility to be introduced in Section 3.3.1. Handover is the enabling technology applied by mobile radio systems to get together communication and mobility. Accordingly, handover related properties are discussed in Section 3.3.2. A special focus will be put on Vertical HandOver (VHO) serving as enabling scheme for system integration in the scope of this work.
To understand the various mechanisms related to mobility, some main components being part of each communication process need to be introduced first. Figure 3.7 depicts involved domains and interfaces:

**User:** A physical person in a certain role that employs services by using network resources. One single person can have different user identities in different roles, e.g., private and business.

**Terminal:** A device that provides access to the network facilities. In addition, it serves as a platform for services and sessions. A built-in user interface allows for input/output of various kinds of information. Using this terminal the user is able to access the network, whereby each information transfer is realized over one or several links.

**Link:** The communication facilities between corresponding entities. A link can have several manifestations, e.g., wired or wireless, depending on the considered network. It is used as description for physical (layer 1) or logical connections (≥ layer 2) between entities of a network.

---

12 Definitions have been derived from discussions within the German VDE/ITG task force 5.2.4 dealing with communication systems and mobility in IP-based networks.
**Point of Access (Attachment):** A device or interface for connecting a terminal to the network. The connection between terminal and network is realized over a *Point of Access* (PoA) that may change, e.g., due to movement of the user/terminal. Its realization depends on the used technology. It may be a plug for a network cable, as well as a base station of a wireless network.

**Network:** Infrastructure providing connectivity and transport related services between PoAs, control entities, and (service) databases. Uplink data arriving at the PoA has to be delivered to the destination by the network and its facilities.

**Service:** Type of information and its characteristics. Key driver of mobile communication has been circuit switched speech service. Future communication supposably will be dominated by packet switched data services with value added services established on top.

**Session:** Set of one or more associations between two or more entities. A session is a realization of a certain service.

The above-introduced terms are necessary for the understanding of the different manifestations of mobility as explained in the following.

### 3.3.1 General Aspects of Mobility

A general definition states mobility as “The quality of being mobile, i.e., to move or be moved easily and quickly from one place to another” [90]. However, this definition is too generic to cope with the various mobility aspects in mobile communication.

There are many manifestations of mobility provided by different communications systems. *Mobility Management* (MM) is the substantial functionality to support changes of the Points of Access. In the following, some main forms of mobility will be presented. The respective definitions are inline with those of fora such as VDE/ITG 5.2.4 (‘Mobility in IP-based Networks’) [2] and ITU-T Study Group 16 (‘Multimedia terminals, systems, and applications’) [16]:

**User (personal) mobility:** The ability of a user to maintain the same user identity irrespective of the terminal used and its network point of attachment. Terminals used may be of different types.
**Service mobility**: The ability of a user to use a particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose.

**Session mobility**: The capability to move an active session between terminals.

**Terminal (Host) mobility**: The ability of a terminal to change its location, i.e., network point of attachment, and still be able to communicate.

*User mobility* refers to a related group of functions, which enable a user to obtain access to services provided via a network, independent of which terminal the user is currently working on. Typically, authentication and authorization procedures need to be applied first. An example of user mobility is use of different mobile phones for which users may carry forward the same identity from one physical device to another. Personalized SIM cards thereby apply to map person and identity.

*Service mobility* is closely related to user mobility. Ideally, a user changes the device used to access services and will face exactly the same service on another device. As an example, users may access emails from their home provider via a web-interface or using a mobile phone with WAP (Wireless Application Protocol) capability. However, if there are any large multimedia attachments to certain emails, it might be possible that the user cannot access them with the mobile phone based access. In this case, user mobility from the web-interface to the mobile is supported, but service mobility is restricted.

*Session mobility* is also related to user mobility in the sense that the user initially starts a session on one device and wants to continue this session on another one. For instance, a user starts a VoIP call using his DSL wire-line attached PC but then decides to leave home and handovers the session to a VoIP capable mobile device with wireless UMTS connection.

*Terminal mobility* is always related to physical movement. It refers to the function of allowing a user’s terminal to change its Point of Access without interrupting service to the user(s) on that terminal. Note that the previous sentence *does not* necessarily mean *seamless* service continuity. Terminal mobility is logically independent of user mobility, although in real networks at least the address man-
agement functions are often required to attach the terminal to the network after switch on.

Besides these mobility aspects, some further important characteristics shall be introduced in the following:

**Seamless mobility:** The user/terminal is able to change the network access point, as he/it moves, without interrupting the current service session, i.e., handovers are possible.

**Nomadic mobility (roaming):** The ability of a user/terminal to change the network access point as he/it moves while the service session is completely stopped and started again i.e., discrete changes of location are done.

**Continuous Mobility:** Movement over a wide area without disconnecting from the network, e.g., 2/3G.

**Discrete Mobility:** Connectivity is provided only within certain areas, e.g., WLAN Hot Spots.

![Figure 3.8: Mobility aspects in this thesis](image-url)
3.3. Mobility & Handover

Scope of this thesis is the investigation of joint terminal mobility and service/session mobility. Since active sessions are assumed, delay impacts shall be minimized, for which seamless mobility plays an important role. Switching between different access networks involves problems arising from discrete mobility (WLAN) and continuous mobility (UMTS). In particular, the Vertical Handover will be addressed as an important mechanism to enable these mobility aspects.

The following section introduces handover aspects in general and vertical handover in particular. Comprehension of these schemes is essential for understanding benefits as introduced by the Hybrid Information System, which will be presented in Section 5.

3.3.2 Handover Aspects

Within literature, many different aspects of handover\(^{13}\) (HO) are described and consequently, various terminologies and definitions can be found. Depending on architecture, procedure, velocity, initiating party, and others, most of them are reasonable and appropriate. The following section takes up main objectives of HO and explains respective properties in detail where necessary.

3.3.2.1 Definition

In general, handover is defined as the act of moving power or responsibility from one person or group to another [90]. In telecommunication, the term handover refers to the process of transferring an ongoing call or data session from one physical resource to another, whereby new parties may be involved and old parties may be released. Accordingly, ETSI and 3GPP define handover as “The transfer of a user’s connection from one radio channel to another (can be the same or different cell)” [109]. Another definition that was also taken over by WINNER states that handover is “The process in which the radio access network changes the radio transmitters or radio access mode or radio system used to provide the bearer services, while maintaining a defined bearer service QoS” [109][116].

\(^{13}\) In literature, the terms handover and handoff are used synonymously. Usually, handoff is more popular in America while handover is the preferred notation in Europe.
3. Integration & Cooperation of Radio Access Networks

All definitions have in common that handover always relates to an ongoing and active connection. While older definitions, such as the US Federal Telecommunications Standard FED-STD-1037C ‘Glossary of Telecommunication Terms’ [143] from 1996 are restricted to circuit switched phone calls, the newer definitions incorporate packet switched connections as well.

3.3.2.2 Reasons for Handover

Probably the most important reason for handover is degrading signal quality due to physical movement in the context of terminal mobility. The underlying cellular concept adopted by all modern mobile communication systems is based on frequency re-use to enhance spectral efficiency\(^{14}\). Transmission power is limited so that only a well-defined area is covered as shown in Figure 3.9. To allow for handover, adjacent cells are designed to overlap each other constituting areas with reception of signals from two or more base stations. Orthogonal transmission resources in time, frequency, or code domain ensure minimal intercell interference. By leaving the original coverage area and entering a new cell during ongoing communication, handover is performed to enable (seamless) service mobility.

![Figure 3.9: Terminal Mobility resulting in Handover](image)

Including mobility as main reason for handover, further metrics apply to be summarized as follows:

\(^{14}\) For a detailed discussion of spectral efficiency in cellular systems, please refer to [157].
• **Better cell handover**: Due to mobility, the user reaches an area in which signal reception from a neighboring cell is better than from the current one.

• **Reference sensitivity level handover**: Reception level of the serving cell drops under a specific required minimum, referred to as the required ‘reference sensitivity level’ The reference sensitivity is the minimum receiver input power measured at the antenna port at which the *Bit Error Ratio* (BER) does not exceed a specific value (usually required BER < \(10^{-3}\)). Note that different systems apply different transmission technologies for which respective thresholds may not be compared on a total basis:
  o For different types of GSM transceivers this limit was defined in [144], e.g., handheld GSM mobiles require a minimum reception level of -102 dBm.
  o UMTS UEs as specified in [145] require -106.7 dBm (CCPCH, etc.) and -117.0 dBm (DPCH) for FDD, while -105.0 dBm (3.84 Mcps) and -108.0 dBm (1.28 Mcps) for TDD mode [146].
  o WLAN IEEE 802.11a/g claims a minimum reception level of -82 dBm (BPSK1/2) [69].

• **Reception quality handover**: The reception quality, usually expressed as *Bit Error Ratio* (BER) or *Packet Error Ratio* (PER), drops under a specific required minimum. Usually, BER and PER are directly related to the *Carrier-to-Interference* (C/I) ratio.

• **Traffic reason handover**: A handover may be triggered due to capacity and traffic reasons, e.g., a cell is heavily overloaded.

• **Speed based handover**: Connections of fast moving users shall be shifted from small (Hot Spot) cells to large cells to avoid frequent handovers respectively dropped connections.

• **Service based handover**: Dedicated services shall preferentially be supported by dedicated cells.
3.3.2.3 Types of Handover

Different HO types are considered according to the Point of Access before and after handover. The following categories as shown in Figure 3.10 are distinguished:

- **Intra-cell Handover**: Switching to another frequency, slot, or code within the same supplying cell due to potential quality degradation or capacity reasons. Intra-cell handover comprises also the switching between different sectors of the same cell. Network connections do not need to be altered [109].

- **Inter-cell Handover**: Handover to a neighbor cell. Contrary to the Intra-cell handover, this type requires network connections to be altered. Further distinctions are made with respect to the logical attachment of the two involved cells:
  - **Intra-BSC/RNC Handover**: Old and new BTS respectively Node B are controlled by the same BSC (GERAN), respectively RNC (UTRAN).
  - **Inter-BSC/RNC Handover**: Handover to an adjacent cell being attached to a different BSC (GERAN), respectively RNC (UTRAN).

- **Inter-system Handover**: Handover between networks using different radio systems, e.g., UMTS – GSM as shown in Figure 3.10 or UMTS and WLAN. Inter-System handover is the most challenging handover type due to different properties of the involved networks. Another notation for Inter-system handover hence is *Vertical Handover* to point out the heterogeneity of the involved networks. Inter-system handover optimization thus is a big challenge and a key topic to be addressed in this thesis. A detailed discussion on Vertical Handover is given in Section 3.3.2.7.
3.3. Mobility & Handover

Considering the Point of Access, the previously introduced handover types described *where* a handover takes place. Within the following, it is shown *how* these types can occur.

### 3.3.2.3.1 Smooth, Fast, Seamless, Ideal Handover

Moving while being covered by different networks without active connection but still being capable of receiving requests is rather related to roaming than to handover. As discussed, the definition of handover incorporates an active (data) transmission. *Smooth* handover denotes to minimization of packet loss, while *fast* handover addresses the requirement for minimum packet delays during the actual HO process. If handover is both, smooth and fast, so that the time span needed to redirect the link is short enough that the application or the user is (almost) unaware of this process, the handover is referred to as *seamless*. 

[Diagram: Different HO Types; exemplary for GERAN and UTRAN]
Accordingly, 3GPP TR 21.905 defines in its *Vocabulary for 3GPP Specifications* that “a seamless handover is a handover without perceptible interruption of the radio connection” [109]. While this definition primarily yields on the radio connection, IEEE 802.21 focuses on the E2E connection. It is stated in [110] that “A *seamless* handover is defined as one that is either an ideal handover or is a handover with some degradation in service parameters that are mutually acceptable to both the user at a terminal and the network that is providing the service”. In contrast to *ideal* handover, the given definitions for seamless HO allow marginal tolerances. Consequently, the requirements for ideal HO are the strictest ones demanding that “An ideal handover across heterogeneous interfaces is where there is no change in service quality, security, and capability as a terminal moves from a source L2 network to a target L2 network” [110].

An important challenge in all these contexts is that no data shall get lost during the handover execution. As long as no path/route update is performed, data to be directed to the mobile is still misrouted to the old serving base station. If the old base station is aware of the new point of attachment of the mobile, seamless handover execution may be supported by tunneling of misrouted data. If tunneling is not supported, all the data will be lost. In spite of dedicated (higher layer) mechanisms to request for re-transmission of lost packets, the time span (delay) might be too big to satisfy the challenges of seamlessness.

Another approach to overcome the problems of potentially misrouted and lost packets and to provide seamless HO is to apply soft and semi-soft HO procedures.

### 3.3.2.3.2 Hard Handover (Break-before-Make)

Moving from one cell to another, the handover process requires the connection to be switched between the two cells. If all the old radio links are removed before new radio links are established, the corresponding handover is referred to as *Hard Handover*, see Figure 3.11.

This case requires special attention to handover latency since the mobile is effectively disconnected during handover. Fast handover signaling mechanisms (fast re-establishment) are required to provide seamless handover. In practice, a handover that requires a change of the carrier frequency (inter-frequency handover) is always performed as hard handover. The same holds for the inter-mode handover from UTRA-TDD to UTRA-FDD and vice versa.
3.3.2.3.3 Soft and Softer Handover (Make-before-Break)

In 3G CDMA based systems, the user can be connected to several base stations simultaneously, combining the data from all transmitters in range into one signal using a RAKE receiver. The *active set* thereby is referred to as the set of base stations to which the terminal is currently connected. Mobile terminals maintaining multiple connections to different cells can perform soft handover. A soft handover happens when there are several base stations in the active set and the terminal drops one of these to add a new one. Accordingly, 3GPP TR 21.905 defines in its ‘Vocabulary for 3GPP Specifications’ that a “soft handover is a category of handover procedures where the radio links are added and abandoned in such manner that the UE always keeps at least one radio link to the UTRAN” [109]. Some definitions as used by the IETF Network Working Group [91] further distinguish between soft handover and ‘Make-before-Break’. However, since both terms define related diversity techniques, no further distinction is applied in this work.

Soft handover, which allows a single mobile to be simultaneously connected to multiple cells, renders the link more robust to fading and thereby enlarges the cell coverage area. The condition that several radio links are active at the same time is also referred to as macro diversity. Normally, soft handover can be used when cells operated on the same frequency are changed. The use of soft handover also facilitates the transfer of traffic from one cell to the next since the mobile enters into communication with the new target cell well before the old cell is dropped. Due to this smooth handover execution, ping-pong effects are reduced as well. However, the benefits inherent in soft handover are critical with regard to setting handover thresholds correctly. If thresholds are too low, soft handover links that are not really needed for call support will be added, thereby generating excess co-channel interference and excess call processing loads. If thresholds are set too high, mobiles that require soft handover links to maintain voice quality will be compromised.

Semi-soft handover is a special case of soft handover. It is used to describe a special micro mobility handover used in UMTS- but also IP networks. During handover within IP networks routing information needs to be updated in order to provide connectivity to the mobile host. IP packets are sent to the old base station until the route is updated. Then all incoming packets are sent to the new base station. There can be a short time interval when the mobile host receives packets both from the new and from the old base station. This is called semi-soft handover.
Softer handover is another special case of soft handover where the radio links that are added and removed belong to the same Node B. In softer handover, macro diversity with maximum ratio combining can be performed in the Node B, whereas generally in soft handover on the downlink, macro diversity with selection combining is applied.

3.3.2.4 Handover control

The decision mechanism for handover control can be located in a network entity or in the terminal itself. The corresponding cases are called Network-Controlled HandOver (NCHO) and Mobile-Controlled HandOver (MCHO), respectively. In most cases, HO is initiated by the controlling instance. In analogy to NCHO and MCHO, it is distinguished between Network-Initiated HandOver (NIHO) and Mobile-Initiated HandOver (MIHO).

If a HO can be planned and is not due to sudden link deterioration, it is possible to trigger a forward HO, where the old BS processes information for potential new BSs. Forward signaling allows for information pushing from the old to potential new serving BSs by building a temporary tunnel. Another notation therefore is proactive (expected) handover.

If an immediate HO becomes necessary (unplanned, unexpected, reactive), no anticipation is possible beforehand. However, the new BS can notify the old BS by means of backbone signaling in order to request for tunneling of misrouted packets (backward HO).
Performing handover control is a critical task. Considering movement of the terminal as shown in Figure 3.9, it is to ensure that triggering (compare Section 3.4) applies early enough to achieve seamlessness. Due to fluctuations in the received signal strengths from both base stations, it is possible that repeated handover between the same two BSs occur – an effect referred to as ping-pong handover. To overcome this problem, a couple of mechanisms are applied: Hysteresis with respect to the received signal strengths of the two base stations ensures HO triggering only, if the new cell’s signal is significantly stronger than the current cell’s one. In addition, dwell time settings ensure a minimum amount of time for which a call is maintained within a particular cell prior to executing another handover.

Obviously, additional parameters such as the speed of the moving terminal have a significant impact on the decision process for handover control. An important contribution of this thesis hereby is valuable support of handover control. Due to link state maps as administered by the Hybrid Information System combined with tracking schemes, it is possible to determine and recommend optimal handover locations. Additional benefit arises from the fact that the Hybrid Information System may not only report on existence of complementary radio systems, but also on local characteristics. Together with a (vertical) handover recommendation, the Hybrid Information System may provide additional context information such as system specific scrambling codes or link adaptation support. Especially hard handovers will benefit by this support, resulting in decreased synchronization and adaptation times and hence, a minimum effective connection’s break. Analytical performance investigations and simulations results on support of handover control by the Hybrid Information System are presented in Section 6 and Section 8, respectively.

3.3.2.5 Layer 2 Handover

The movement of terminals between points of access of the same subnet usually is managed by Layer 2 (L2) protocols. A subnet is defined as “a logical group of connected network nodes” [91] sharing a common network mask (in IPV4) or a network prefix (in IPv6). In practice, all kinds of intra-cell handovers and some kinds of inter-cell handovers are handled exclusively by L2 for which L2 HO is also referred to as radio handover or cellular handover. It is either completely transparent to the routing at the IP layer or it appears simply as a link layer re-
configuration without any mobility implications. Since the entire HO execution can be executed on L2 basis, all relevant information about ongoing user connections can be maintained. This includes aspects like authentication or security parameters making re-negotiation obsolete.

Within this thesis, L2 handover is of particular interest. A special challenge thereby derives from the fact that vertical handover involves the incorporation of different air interfaces. Especially synchronization and detection mechanisms play an important role. Investigations as in [101] have shown that L2 handover execution contributes significantly to the overall HO latency. The impact was shown to get even stronger the more users contend for access. Considering the IEEE 802.11 air interface, it is further stated in [106] that “the principle overhead is due to L2 properties”.

Classical handover execution applies L2 handover followed by L3 handover afterwards. Newer proposals focus on quasi-parallel L2 and L3 handover to reduce the resulting delay. If handover can be anticipated, L3 handover can already be triggered or prepared prior to L2 handover. Concepts as proposed in [151] define pre-warming zones being candidate future APs/BSs for handover. Context transfer by means of backbone signaling hence reduces the overall handover delay to the time span needed for L2 HO execution.

The Hybrid Information System as part of this work helps reducing L2 handover delay. In addition, based on respective short- and mid-term data, prediction support is given allowing for anticipation of user movement and definition of pre-warming zones.

**3.3.2.6 Higher Layer Handover**

The network layer (L3) is the highest network dependent layer being responsible for setting up, operation and termination of network connections in general, and routing in particular. During a network handover (L3 handover), the terminal associates to a new subnet and a new routing path needs to be established. Further, authentication and security procedures need to be triggered as well as renegotiation of QoS parameters.

Though higher layer handover does only play a minor role in the scope of this thesis, some mechanisms and protocols are shortly discussed in the following for
the sake of completeness. L3 handover in IP based networks is often handled by *Mobile IP* (MIP). In order to reduce handover latency, MIP managed macro mobility can be supplemented by micro mobility protocols such as Cellular IP [94] or HAWAII [95] that provide fast handover processing within smaller domains or subnets transparently to MIP. An interesting approach for integrated macro/micro mobility concepts has been published in [96].

Mobile IP (for IPv4) [93] introduces new entities such as *Home Agent* or *Foreign Agent*. Standard IP routing is applied to support mobility so that no other changes need to be implemented. A temporary *Care-of Address* serves as connection end-point for the terminal. Datagrams arriving at the original home address can be tunneled to the Care-of-Address allowing for transparent connectivity of roaming users. Due to limitations of MIP based on IPv4, enhancements became necessary resulting in MIP based on IPv6 [97][98]. Terminals apply address auto-configuration to acquire their care-of address mitigating the need for Foreign Agents. A comprehensive description of MIPv4/v6 related topics is given in [99].

In addition to L3 handover, further mechanisms exist that could be subsumed as ‘higher layer handover’. From the ISO/OSI model perspective, handover can be considered as a reconfiguration or ‘exchange’ of specific layers. L2 handover hence is interpreted as a reconfiguration of the physical layer and the data link layer, while L3 handover further affects reconfiguration of the network layer. Ideally, higher layers do not recognize replacement of lower layers meaning that the handover process is transparent. From this point of view, session mobility as introduced in Section 3.3.1 can also be interpreted as higher layer handover, i.e., ‘session handover’. A respective enabler thereby could be the *Session Initiation Protocol* (SIP) [100].

### 3.3.2.7 Horizontal & Vertical Handover

Performing handover from any source to target system both of which applying same technologies and relying on same specifications is referred to as *Horizontal HandOver* (HHO). If handover is triggered to another system using a different technology, the notation *Vertical HandOver* (VHO) applies.
Vertical Handover hence always comprises the involvement of at least two different systems. Accordingly, one refers to this kind of handover as inter-system handover to express that it is a “handover between networks using different radio systems, e.g., UMTS and GSM” [109].

According to the supported coverage of involved systems, it is distinguished between upward and downward VHO. Upward VHO denotes the switching from a system with smaller cell sizes and usually higher bandwidth to a wireless overlay with larger cell sizes and usually lower bandwidth per unit area. Downward VHO is the handover in the other direction, respectively. Figure 1 depicts both handover types.

Compared to horizontal handover, vertical handover introduces new degrees of freedom. For example, it is possible that a decision unit triggers VHO execution due to QoS aspects, though the actual link quality in the current cell is excellent. If namely another vertical system with a multiple of offered data rate is available, the decision space is no longer restricted to sole link parameters.

Beyond this background, origins for handover may be further distinguished into radio related handovers and service related handovers. While better cell handover, sensitivity level handover and reception quality handover are radio related handover reasons, traffic reason handover, speed based handover and service based handover are service related handovers.
As a rough classification, horizontal handovers fall mainly in the category of radio related handovers, while vertical handovers subsume service related handovers. For more information on HHO and VHO, please refer to [82] and [83].

It is worth noting, that one needs to distinguish between horizontal/vertical and L2/L3 handover. While the first couple refers to involved technologies, the second couple addressed involved layers and logical affiliations. Due to the encapsulated service principle of the ISO/OSI model [84], the IP layer sees network interfaces and IP addresses rather than specific technologies. Thus, horizontal and vertical handovers may or may not be noticed at the IP layer.

3.3.2.7.1 Particular Vertical Handover Properties

Since VHO decisions derive from an enhanced decision space, some particular properties are shortly discussed in the following section.

**Time criticality**

Considering mobility and timing aspects, the downward VHO is much less time critical, since the terminal may sufficiently long rely on its old connection during the handover process. The upward VHO instead needs to take place in time, otherwise the user may have moved out of the coverage area of its old serving (WLAN) AP before the procedure has been completed. Within this thesis, both downward and upward VHO are investigated. It will be shown that for specific requirements, e.g., throughput optimization, downward VHO turns out to be time critical as well. This is inline with previously published results by the author in [85].

**Transparency**

Signal reception quality is likely to change due to various reasons. Mobile radio systems encounter this problem by applying sophisticated mechanisms such as power control, link adaptation, and handover. All of these measures have in common that dedicated boundaries, e.g., minimum throughput requirements, are to be kept. The overall aim is to realize transparent service provisioning to higher layers in terms of e.g., constant supported bit rate. However, unlike for horizontal handover, vertical handover comprises switching between heterogeneous systems with completely different framework conditions. As such, the immense discrepancy e.g., with respect to supported bandwidth can no longer be balanced by lower layer adaptation mechanisms. In addition, it is not possible to
guarantee the same levels of QoS across different systems, for which renegotiation becomes necessary. All this results in decreasing transparency for VHO compared to HHO.

**Decision Space**
Since horizontal handovers fall mainly in the category of radio related handovers, it is comparatively easy to define metrics for handover decision. Respective triggers are presented in Section 3.4. Vertical handover however, introduces additional degrees of choice, such as QoS, costs or service availability. Being of very different nature, objective comparison is difficult. Algorithms applied for HO decision hence need to apply rating of input parameters. User defined policies will play an important role at this.

**Business Aspects**
In addition to technical innovations, application of heterogeneous transmission technologies requires new business models, too. New cost structures in terms of *Capital Expenditures* (CAPEX) for investments and *Operational Expenditures* (OPEX) for operation, administration, and maintenance need to be considered. Billing among several involved systems and operators becomes a rather complex task. Classical time or volume based billing schemes cannot that easily be over-taken, for which questions like the following ones need to be answered [107]:

- Where to meter the different traffic measures?
- How to accumulate them in a technology independent way?
- How to combine the costs caused in the networks of the different network technologies?
- How to achieve one bill when different network operators contribute?
- In which of the domains shall this combination be achieved?

**3.4 Trigger**
The widespread seen need for link layer information to upper layers is clearly expressed by a number of (recently) established standardization groups, especially within IETF and IEEE. Key driver here is the intention to speed up (vertical) handover execution since link layer events are expected to anticipate user (mobile terminal) movement and to prepare the mobile terminal and network in advance. Existing L3 protocols such as Fast MIPv6 [108] have been designed to incorporate link layer notifications.
3.4.1 Definition & Classification

Whenever handover decisions are to be taken, respective algorithms need to rely on particular data referred to as *trigger*. Depending on the origin and destination of triggers, the following distinction is herewith introduced: Triggers having been fired by a logical peer entity (different unit, same layer) usually serve for remote information provision. As such, context transfer is intended. Due to the logical information flow between two entities of the same layer, these kinds of triggers are labeled as *horizontal triggers*.

In contrast to this, notification messages from lower to higher layers are labeled as *vertical triggers*. In fact, many specifications inherently refer to *vertical* triggers when addressing triggering. Vertical triggers usually are unidirectional, being fired from the lower to the higher of two adjacent layers. However, some information flows may also skip intermediate layers when reporting changes. An example for this is the information flow between PHY (layer 1) and RRC (layer 3) in UMTS.

In general, (vertical) triggers are pieces of information that indicate changes of setup or surrounding conditions. A commonly used definition within IETF says that “An L2 trigger is an abstraction of a notification from L2 (potentially including parameter information) that a certain event has happened or is about to happen” [92]. Many discussions have taken place to define a commonly agreed picture of triggers, especially within IETF (TRIGTRAN, SEAMOBY, PILC, ALIAS), IRTF (MOBOPTS) and IEEE (802.21 Media Independent Handoff Working Group).

Particular benefit with respect to handover latency is given, if L2 trigger allow for initiation of L3 handover before L2 handover has completed, e.g., movement anticipation for Fast Handover Protocol for MIPv6 is based on L2 triggers. While the question of the delivery mechanism, e.g., via a standardized API, remote procedure call, or others, is commonly seen secondary, the question of what information should be passed between L2 and L3 is intensively discussed. The predominant opinion is that L2 triggers should turn out to be *generic* and *abstract*, and not specific to any particular link layer. They should rather represent generalizations of link layer information available from a wide variety of link layer protocols [91]. Proposals for this as favored within IETF and IEEE are
Triggers subsequently only indicate ongoing changes. Specific radio characteristics herewith are hidden to higher layers providing an ISO/OSI conform and transparent operation while simultaneously allowing for anticipation of higher layers.

3.4.2 Decision Criteria

To allow for generation of triggers, L2 is dependent on measurement reports provided by the physical layer. Within the IST project MIND [46], the term physical-based triggers was introduced to refer to L2 triggers generated as response to L1 reports. In addition, MIND defined algorithm-based triggers to refer to L2 triggers generated due to algorithms running in the data link layer, see Table 3.2.

Table 3.2: L2 Trigger generation due to different origins

<table>
<thead>
<tr>
<th>Physical-based triggers</th>
<th>Algorithm-based triggers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal Strength (RSSI, RSCP, RPI)</td>
<td>HO Ping-Pong avoidance by means of hysteresis</td>
</tr>
<tr>
<td>Interference level</td>
<td>QoS violation (e.g., in/-decreasing PER)</td>
</tr>
<tr>
<td>Carrier-to-Interference Ratio (C/I)</td>
<td>Connection Admission Control status</td>
</tr>
<tr>
<td>Bit Error Ratio (BER) / Packet Error Ratio (PER)</td>
<td>Connection Forwarding (CAC &amp; CF)</td>
</tr>
<tr>
<td>Not explicitly addressed within MIND:</td>
<td>Location based trigger</td>
</tr>
<tr>
<td>#HO, #Retransmissions (ACK/NACK)</td>
<td>Velocity based trigger</td>
</tr>
<tr>
<td># Dropped calls or packets</td>
<td>A priori-knowledge based trigger</td>
</tr>
<tr>
<td>Delay, HO-latency</td>
<td>Service availability trigger</td>
</tr>
<tr>
<td>Current window size (ARQ)</td>
<td>Grade of Service</td>
</tr>
</tbody>
</table>

While the description above presumes homogeneous system environments with scope on horizontal handover, it is explicit concern of this thesis to consider heterogeneous system concepts. It was already stated in the previous section that vertical handover triggering requires special treatment due to the expanded decision space meaning that it is pointless to compare total values of physical-based triggers of different systems, see definition of sensitivity level handover in Sec-
3.4. Trigger

Hence, prior to firing a HO recommendation to L3, L2 should implement sophisticated evaluation logic. Respective research is currently undertaken within WINNER that defines a heterogeneous network environment with different radio interface modes.

Since several handover triggers can happen at the same time it is proposed that the decision algorithm should be supervised by a Joint Arbitration Algorithm to prioritize the individual algorithm and optimize the final handover decision [112]. The overall WINNER L2 handover architecture is given in Figure 3.13.

The Hybrid Information System as proposed within this work is integral part of the WINNER proposal, see Section 5.6.3. In addition, information provisioning to the joint arbitration algorithm with respect to further non-WINNER systems is possible.

The implementation of the actual joint arbitration algorithm depends on given requirements. An algorithm for optimization of inter-system handover between UMTS and GSM that targets on reduction of compressed mode overhead and avoidance of unnecessary handover is presented by Forkel in [113]. The decision criterion based on which an appropriate classification of Node Bs takes place is the complementary distribution function of the Received Signal Code Power (RSCP) within the cell area. Depending on this classification, different thresh-
olds for CM application and triggering are defined for ‘inner’, ‘transit’ and ‘outer’ cells.

Investigations on RRM principles that are more general have been undertaken by Furuskär [115]. Since the capability to handle services typically differs between systems, the allocation of services affects the overall capacity. As a result, either service allocations should be extremes, i.e., isolated services in different systems, or they should be equal to all systems characterized by the relative efficiency. Anyhow, considering also radio resource costs, initial attempts are made to show that performance improves the more information is available.

A particular contribution of this thesis is the definition of a framework to provide inter-system information transfer based on which subsequent joint arbitration algorithms can rely. Within its prototypical implementation, triggers for VHO as generated by the Hybrid Information System consider decision criteria in the following order:

1. user preferences,
2. user location (Location Based trigger $\rightarrow$ Algorithm-based trigger),
3. system disposition (Service availability trigger $\rightarrow$ Algorithm-based trigger),
4. current link quality (RPI $\rightarrow$ Physical-based trigger),
5. station movement (Velocity based trigger $\rightarrow$ Algorithm-based trigger).

Especially the consideration of user preferences within the trigger decision-making process is an important subject supported by HIS. Applying user preferences extends purely physical-link based handover algorithms by policy-based management. This is important if e.g., business aspects shall be considered. Figure 3.14 exemplarily depicts the decision-making process, within which HIS deliberately balances user preferences with given link conditions prior to generating VHO trigger.
Prioritization of triggers as controlled by the joint arbitration algorithm particularly applies policies. Unless stated otherwise, the algorithm implemented in the Service Control Unit of HIS applies prioritization according the orders (1)-(5) given above. User preferences were set to ‘handover to WLAN whenever possible’ (1). Upon request, due to incoming events, or on a periodic time scale, HIS checks whether WLAN is available for a station at a given position. Prior to generating the trigger, it is checked whether the target system supports the requested service (3). Depending on the link quality in the target system, additional context information such as initial PHY-Mode proposals may be generated (4). If all requirements (1)-(4) are fulfilled, station movement (5) can be exploited to anticipate future handover decisions, define pre-warming zones or prepare planned HO execution.

**Figure 3.14: Policy based trigger generation considering user preferences**
Localization Techniques & Principles

Content

4.1 Localization & Positioning ................................................................. 102
4.2 Basic Localization Principles .......................................................... 110
4.3 Cellular Localization .................................................................. 116
4.4 Satellite Localization ................................................................. 126
4.5 Accuracy & Precision ................................................................. 134
4.6 Summary ............................................................................... 137

Keywords: Localization, Positioning, Reliability, Enabling Technologies

Localization and positioning in mobile radio networks become more and more important since they provide inherent means for value added service provision. Thus, these techniques do not only represent a value of their own, e.g., for people who want to be aware of their current position, but will take over the role of a key technology based on which new services will operate. Different manifestations of Location Based Services (LBS) promise to become an important market.

The role of positioning as enabling technology justifies a deeper reflection of its properties. When talking about localization, people most obviously associate satellite based systems. However, this is not in the focus of this work. Instead, localization support inherently provided by means of mobile radio is considered. Nonetheless, hybrid solutions will also play a significant role in the future of positioning for which a short introduction to non-cellular positioning schemes is given as well.

The following chapter provides a general overview of localization in Section 4.1. Besides an introduction to localization methods and applied techniques, possible metrics to classify localization systems are discussed in Section 4.2. Sections 4.3 and 4.4 present concrete realization schemes of cellular and non-cellular local-
ization. Particular attention should be paid to the definitions of accuracy and precision in Section 4.5. These terms represent abstract properties of concrete positioning techniques and serve as input parameters for analysis and simulation. A summary on different (hybrid) positioning techniques is given in Section 4.6.

4.1 Localization & Positioning

Generally speaking, localization is the determination of the locality (position) of an object. Being derived from the Latin word ‘locus’ (lieu, location, place, position), the original meaning is to fix or to narrow down the place of an event or object. However, depending on the field in which localization is applied, different contexts apply. In economics, localization is a way to adapt products for non-native environments. In mathematics, localization is a certain technique in abstract algebra. In acoustics, sound localization describes how our ears find the direction of a sound source. In telecommunication, localization is a technique for determining the location of a user/phone.

Further synonyms for ‘localization’ commonly used are ‘positioning’ or ‘location’. Since ‘location’ is both, a synonym for the act of localizing as well as a synonym for the statement of a place, it is not further used in the first context. Similar to ‘localization’, the term ‘positioning’ is also employed in more than one sense. In marketing, positioning is a technique related to the creation of an image or identity for a product, brand, or company. It is the ‘place’ a product occupies in a given market as perceived by the target market. More generally, ‘positioning’ is a term used for the careful placement of objects, and in particular, by the use of precise navigation (for example, in the notation ‘Global Positioning System’).

However, applying localization and positioning in the context of telecommunications and mobile radio networks, both notations refer to the act of localizing or state of being localized. For this, both terms are used synonymously within this work.

4.1.1 Localization – What for?

Being aware of the own position is of substantial interest, comparable to time awareness. The accuracy required depends on the action to be carried out or the
information requested. For the \textit{time domain}, this could mean that it is sufficient to be aware of the current date, e.g., for birthday greetings. However, if a meeting is scheduled, a more precise date and time is necessary including hour and minute of the appointment. Similar considerations hold for the \textit{space domain}. Obtaining information on the weather forecast requires accuracies on region or country level, while reaching a specific venue requires more detailed address information.

A further parallel between time and space domain is, that information usually is evaluated relatively: Having an appointment at a dedicated point of time in the future implies the necessity of knowing the current time, too. Finding a place based on its address information implies awareness of the own position, respectively.

\subsection*{4.1.2 Location Based Services}

In general, location information is important, while the degree of required resolution varies. Positioning is a precondition to provide support in a number of fields. Examples are traffic information and navigation (What is the best way to travel from A to B?), location visualization (Where am I?), leisure information (Where is the nearest restaurant?), emergency services (Where to shovel snow to find avalanches victims?) or people/goods/fleet tracking (Where are the trucks of my company?).

Parts of these tasks are summarized as \textit{Location Based Services} (LBS). A widely adopted definition states LBS as “the ability to find the geographical location of the mobile device and provide services based on this location information” [193]. Hence, positioning is not an end in itself but serves as enabling technology for LBS. Application areas of LBS are manifold and comprise:

\begin{itemize}
  \item Safety/Emergency Services
    \begin{itemize}
      \item E-911 and others (see Section 4.1.2.1)
      \item Disaster Scenario
    \end{itemize}
  \item Information Services & Telematics
    \begin{itemize}
      \item Traffic information, navigation assistance, yellow pages, travel/tourism services
    \end{itemize}
  \item Enterprise Services
    \begin{itemize}
      \item Vehicle & people tracking, logistic systems, fleet & workforce management
    \end{itemize}
\end{itemize}
• Consumer Portal Services  
  o Services for delivery of local news, weather, shopping or traffic information  
• Crime/Terror Prevention and Fighting  
  o Observation  
  o Tracking of daytime release prisoners while on parole  
• Military Deployment  
• Location Based Networking  
  o LBS Charging  
  o LBS Multicast, Addressing

Obviously, LBS entail high economic potentials (to be addressed later on). However, the driving force for initial definition of LBS capabilities ascribes to non-profit safety and emergency services. Studies as discussed in [194] point out that 60% of the people reporting an emergency are not able to provide a precise description of their position. Considering further that a mobile is used within 98% of these emergency calls was the reason for which actions were taken by regulation authorities: Operators were forced to provide means for localization support. Latest emergency incidents approve this ruling: Seventy-one lost people could be rescued in Sri Lanka after the flood disaster in the Indian Ocean in December 2004 after tracking based on cellular localization techniques was successful.

4.1.2.1 Background

The foundation stone of Location Based Services was laid in 1996 by the US Federal Communications Commission (FCC). The FCC’s wireless 911\(^{15}\) rules seek to improve the reliability of wireless 911 services. Location information shall allow assisting wireless 911 callers much more quickly. The initiative, referred to as ‘Enhanced 911’ (E911) [195], requires all wireless phone providers to develop a way to locate any phone that makes a 911 emergency call.

The wireless E911 program is divided into two parts – Phase I and Phase II. Phase I started in April 1998. It requires carriers upon request by a local Public Safety Answering Point (PSAP) to report the telephone number of a wireless 911 caller and the location of the antenna that received the call. Phase II started in

\(^{15}\) 911 is the official national emergency number in the United States and Canada. Under a federal law enacted in 1999, 911 will replace all other emergency telephone numbers in the US.
October 2001 and is meant to be completed by the end of 2005. It requires wireless carriers to provide far more precise Automatic Location Information (ALI), within 50 to 100 meters in most cases. To comply with E911, vendors are exploring several RF techniques, including antenna proximity, angulation using phased antenna arrays, lateration via signal attenuation and signal propagation delay\textsuperscript{16}, as well as GPS-enabled handsets that transmit their computed location to the cellular system. The underlying principles of localization are explained later on in Section 4.3. To meet the FCC requirements, positioning must be accurate to within 50 m for 67\% (150 m / 95\%) of calls with handset-based solutions, or to within 100 m / 67\% (300 m / 95\%) with network-based solutions [195].

Ongoing efforts by the European Commission target on establishing a similar program in Europe referred to as E112. However, regulations here are expected to be less restrictive.

### 4.1.2.2 Economic Prospects

Location Based Services are expected to be to the benefit of both, customers and network operators. While customers will have greater personal safety (e.g., emergency services), more personalized features (e.g., individual information supply) and increased communication convenience (e.g., detection of nearby online gaming partners), the network operators will open up new markets due to enhanced service portfolios. Primary location based schemes for cellular networks, such as location based billing (‘Homezone’ concept of ViagIntercom/O2), have been launched in 1999. New providers are expected to enter into the market to complement operators’ service offers.

Similar to many other promising new technologies, LBS went through the classical hype cycle when being introduced. The peak was probably reached in 2000/2001, when LBS were announced to serve as new killer application for mobile-commerce by 2004. However, apart from a few realizations, no mass-market could be opened so far. Reasons for this are manifold and comprise e.g., initial hesitation by operators balking high investments in location techniques as well as non-acceptance by the users being either swamped with new services or simply not willing to pay for. The latter comes along with failure of WAP services that initially were chosen to provide LBS.

\textsuperscript{16} Within literature, signal propagation delay is also referred to as ‘time-of-flight’.
Nowadays, situation has changed, for which LBS is poised to make a comeback - albeit without the flash and hype. Operators are building up new infrastructural elements in the scope of 3G deployments anyway, including e.g., Location Measurement Units (LMU, see Section 4.3.3). The E911 (E112) legislation requires the ability to pinpoint the location of a cell phone making the next step to provide LBS based on inherently available information consistent and logical to generate return of investment. Finally, customers show increased willingness to use (and pay for) additional services in addition to speech telephony only, see Figure 4.1 [160].

Figure 4.1: Consumer disposition to spend money on value added services
Source: The Yankee Group 2004 Mobile User Survey [160]

Today, LBS are seen as a means to raise the Average Revenue Per User (ARPU). By offering value added services, the demand for higher-priced data services is expected to rise as well. This is also expressed by a statement of an analyst from ABIresearch\(^\text{17}\) saying: “While carrier deployments are escalating globally, the real money is in the services” [164]. A respective ABI study from 2004 on the LBS market [165] anticipates a total revenue of more than $3.6 bil-

\(^{17}\) Allied Business Intelligence Research (ABIresearch, www.abiresearch.com) executes globally operating technology market research in wireless, automotive, semiconductors, broadband, and energy.
lion for handset based LBS by the end of the decade. While the total amount differs, the given dimensions are inline with other studies e.g., by the Yankee Group\textsuperscript{18} [166], that predicts a volume of more than $4 billion in 2007 in Western Europe. This is even outbidden by the global revenue for telematics LBS services, which is expected to exceed $5 billion by 2009. In addition to European countries and the United States, Asian countries like Japan also expect location-based applications to go through further evolution [167]. Putting human users in the center and tracking the dynamic movement of people and changes in the living space is expected serve as basis for new sophisticated LBS.

It worth noting that the previously discussed prognoses need to be handled with care concerning the \textit{absolute} amount of revenue. Nonetheless, beyond the background that LBS have already gone through the classical hype cycle, they identify the potential of new services based on location information. Apart from the fact that the technical framework is being established, user disposition to adopt these new services seems to be given. If operators manage to establish adequate business models, this may result in a promising trend towards LBS.

\subsection*{4.1.2.3 Privacy}

In general, provisioning of dedicated services always requires specific information, but obviously, this entails the risk of misemployment. This holds in particular for LBS that indispensably entail the need for positioning. Two important demands thereby arise: On the one hand, users request for services that are more sophisticated but on the other hand, they want to be sure that there is no misuse of personal data. At this stage, using a mobile while switched on and moving makes the network tracing a user’s way in order to support handover. Whereas positioning hereby is rather fuzzy, sophisticated LBS need to apply localization methods with higher granularities. Position information, especially tracking, allows for monitoring and observing individuals, deriving mobility profiles and other personal patterns.

The attendance to adopt LBS indicates that users generally are willing to accept the resulting trade-off. However, leaving a certain degree of privacy control with

\textsuperscript{18} Yankee Group (http://www.yankeegroup.com/) is a worldwide operating consulting company with areas of expertise in telecommunications and wireless/mobile communications; IT hardware, software and services; consumer technologies, media and entertainment
the user is of essential importance. Due to a study of the Cahners In-Stat Group [168] more than 2/3 of respondents said it would be extremely important to opt-in, or to give permission to have their location tracked. More than 80 percent of the users demand for the ability to turn the location-tracking capability of a wireless phone on or off at will. In addition, more than 85% found it extremely important to be able to control how their location information is used by service providers and others.

Thus, in addition to personal privacy control, transparency of data handling is a big concern. The European Commission has met these requirements in its Directive 2002/58/EC (Directive on Privacy and Electronic Communications) [169]. Besides regulating many aspects of electronic communication, e.g., ‘unsolicited communications’ (Article 13) the general modus operandi with respect to location data is explicitly covered by Article 9. The most important regulations can be summarized as follows:

1. Location data may only be processed when made anonymous, or with the consent of the users.
2. Processing is restricted to the extent and for the duration necessary for the supply of a value added service.
3. The service provider must inform the users, prior to obtaining their consent, of the type of location data that will be processed. In addition, purposes and duration of the processing must be clear and whether the data will be transmitted to a third party for providing the value added service.
4. Users shall be given the possibility to withdraw their consent for the processing of location data at any time.
5. Once the user agreed on processing his location data, he must continue to have the possibility of temporarily refusing the processing, using a simple means and free of charge.
6. Processing of location data must be restricted to special parties and must be restricted to what is necessary for the purposes of providing the value added service.

---

19 Ongoing discussions within the EU target on (location) data storage and computing for crime and terror fighting. Final decisions have not been taken at the time of writing this thesis.

20 Within this EC directive, location data always refers to “location data other than traffic data”.

---
Standardization bodies such as IETF or 3GPP have taken up this regulation and recognized the need for privacy protection. Within IETF, the *Geographic Location/Privacy* (geopriv) Working Group [170] addresses user privacy from a higher layer and application point of view and 3GPP even provides a whole framework with respect to ‘Enhanced support for User Privacy in location services’ (3GPP TR 23.871, [171]). Starting with Release 5, additional privacy-supporting mechanisms have been introduced, e.g., *Service Type Privacy* allowing for different privacy settings for individual services. In addition, five privacy settings according to Table 4.1 have been specified in the ‘Functional stage 2 description of Location Services (LCS)’ (3GPP TS 23.271, [172]).

**Table 4.1: Privacy settings and strictness in 3GPP**

<table>
<thead>
<tr>
<th>Privacy Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>loose</td>
<td>Positioning allowed without notifying the UE user</td>
</tr>
<tr>
<td>↑</td>
<td>Positioning allowed with notification to the UE user</td>
</tr>
<tr>
<td>↓</td>
<td>Positioning requires notification and verification by the UE user; positioning is allowed only if granted by the UE user or if there is no response to the notification</td>
</tr>
<tr>
<td>strict</td>
<td>Positioning requires notification and verification by the UE user; positioning is allowed only if granted by the UE user</td>
</tr>
<tr>
<td></td>
<td>Positioning not allowed</td>
</tr>
</tbody>
</table>

Operators try to seek the users’ confidence by setting up self-defined rules. UK Mobile Operators for instance issued a so-called *Privacy Management Code of Practice* that sets the guidelines on how personal tracking services should be operated and how safety and privacy of mobile phone users is to be protected. It is therein distinguished between two types of location services: A) *Active Services*, where the end user initiates the location request and B) *Passive Services*, where a third party requests for localization of an individual. Service type privacy as discussed earlier allows different privacy settings for either type. Common practice today (in Germany) is that people explicitly need to agree prior to being localized.

Further related work addresses joint location security and privacy. Frameworks with a cryptographic approach of an authorized anonymous-ID-based scheme [148] have been proposed along with algorithms for location disclosure-control
[149]. Other approaches such as [150] are based on frequently changing pseudonyms and [151] proposes a Location Aware Service Broker that takes over the role of a proxy to hide user identities to external providers.

In summary, LBS are an attractive but also sensitive new field. Fact is that far less comfort to the end user is feasible without exploitation of location information. Regulative actions, legislation, and self-commitments are important means to provide a path for LBS. However, supervision is necessary to avoid potential illegal and unethical use of information concerning individuals’ whereabouts.

4.2 Basic Localization Principles

Localization is based on analysis, evaluation and interpretation of appropriate input parameters. Most of them are related to exploitation of physical characteristics being measurable in a direct or indirect way. Other potential methods being based on e.g., cognition or intuition are not further considered in this work.

From a physical localization point of view, there are three principle techniques to be distinguished:

1. Triangulation/Trilateration:

In trigonometry and elementary geometry, triangulation is the process of finding a distance to a point by calculating the length of one side of a triangle formed by that point and two other reference points, given measurements of sides and angles of the triangle. Such, trigonometric methods are used for position determination. It can be distinguished between

- distance-based (tri-)lateration (example: Global Positioning System, GPS), and
- angle- or direction-based (tri-)angulation (example: phase-sensitive antennas).

For distance-based lateration, the position of an object is computed by measuring its distance from multiple reference points. Possible methods for measuring comprise direct measurements by physical actions or movements, time-of-flight measurements by taking the time it takes to travel between the object and a cer-
tain point at a known velocity and attenuation measurements by exploiting path-loss properties.

2. Proximity:
Proximity is based on the determination of the place of an object that is nearby a well-known reference place. Again, one distinguishes three fundamental sub-methods:

- Registration of a physical contact, for example piezoelectric pressure or contact sensors, capacitive transducers etc.
- Monitoring of (Radio) Access Points. Here, it is evaluated whether a terminal is in the range of one or several APs.
- Monitoring of automatic authentication systems such as credit card terminals, access systems, bar-code scanners, system logins etc.

3. Pattern Recognition:
Within methods that apply pattern recognition, a further separation into

- optical pattern recognition (scene analysis) and
- non-optical pattern recognition

can be taken. With the scene analysis, simplified views of an observed scene are used for the representation and comparison of pictures, for example the horizon line captured with a camera. With the static scene analysis, an allocation of the respective object to pre-defined database objects with well-known positions takes place. In contrast to this, a comparison of sequential pictures is done for the differential scene analysis in order to determine the current position of an object. The differences of the pictures correspond to the movements of the object that is traced.

The advantage of pattern recognition is in the bare observation, without need for determination of angle- or distance parameters. However, changes of the actual scene (e.g., objects or landscape) require a change or a new modeling/update of the underlying database.

Similar to scene analysis, non-optical pattern recognition techniques also apply mapping techniques of dedicated parameters to samples stored in a database. Contrary to the scene analysis, the input usually does not consist of pictures
taken by a camera, but any arbitrary other physical quantity to be evaluated, e.g., echoes in ultrasonic diagnostic.

For both recognition techniques, optical and non-optical, dedicated mapping schemes are applied such as the Database Correlation Method based on Hidden Markov Models, see Section 4.3.5.

4.2.1 Classification of Localization Techniques

Different localization principles may be applied to gain position information with respect to an object that is to be tracked. However, the various concepts open a variety of differentiating factors. Since the scope of this work is concentrated on mobile radio networks, the subsequent classification is derived according to the active network elements in the localization process. Five different categories can be distinguished:

- Network-based,
- Terminal-based,
- Network-assisted,
- Terminal-assisted, and
- Foreign System based/assisted.

While the first four techniques mainly rely on system inherent signal exploitation, the last category applies additional non-specific mobile radio techniques in order to perform localization.

*Network-based positioning*

If all necessary measurements are performed by the network (by one or several base stations), the localization is referred to as ‘network-based’. The measurements usually are sent to a common location centre being part of the core network. This centre takes over the final computation of the terminals’ positions. The advantage is that no changes to the terminals are necessary and legacy devices can be integrated. However, the technique fails if the terminal to be located is in idle mode and does not transmit any information. Beyond that, necessary signaling introduces additional load to the network.
Terminal-based positioning
In the terminal-based\(^{21}\) localization approach, the terminal accounts for position determination. Therefore, base stations need to transmit on a regular basis. If no active communication is established, beacon signals need to be conveyed to enable all users in the cell to perform autonomous localization at arbitrary times. Depending on the sophistication of the terminal-based localization, the base station might need to supply additional information, like its own position. Disadvantages of terminal-based localization obviously are given by increased terminal complexity. Increased challenges with respect to calculation power and equipment lead to the assumption that this method is only partly applicable for legacy terminals.

Network-assisted positioning
Similar to terminal-based positioning, network-assisted positioning implies that the final calculation of the terminal’s position is taken over by the terminal. Thus, the same preconditions as discussed earlier apply. The difference is that possible assistance data is sent by the network. This can be done either on request or in a push-manner.

Terminal-assisted positioning
The fourth category, called terminal-assisted\(^{22}\) localization, is a hybrid implementation of the other methods. The terminal hereby measures reference signals of incoming base stations and provides feedback reports to the network. The final position computation takes place in a central location centre within the network. However, explicit measurement signaling introduces additional load to the network. Furthermore, the evaluation of the position is delayed compared to the terminal-based implementation. The major advantage is the possibility to use existing measurement reports as already specified for UMTS [61], see also Section 2.1. Hence, terminal-assisted positioning can be based on current specifications while only minor changes become necessary. Besides this, if respective reports are exploited that are conveyed to the base station anyway, e.g., in the context of power control, the previously discussed disadvantage of additionally introduced overhead is not given anymore.

\(^{21}\)‘terminal-based’ and ‘mobile-based’ may be used synonymously.

\(^{22}\)‘terminal-assisted’ and ‘mobile-assisted’ may be used synonymously.
Foreign system based/assisted positioning
The last category, foreign system based/assisted localization, differs from the
other three categories by exploiting additional metrics whose origin is not the
actual mobile radio system itself. Methods to be applied comprise radar location
techniques or satellite navigation systems. Furthermore, inter-system solutions
incorporating localization based on mobile radio network techniques jointly ap-
plied with foreign system techniques belong to this category. Depending on the
degree of support, a distinction in foreign system based and -assisted can be
made.

While the previous five classifications are based on the active network element,
another classification is based on the measurement principle [191]. It is proposed
to distinguish three categories:

- Multilateral (one terminal $\rightarrow$ X base stations),
- Unilateral (X base stations $\rightarrow$ one terminal), and
- Bilateral (one base station $\leftrightarrow$ one terminal).

Multilateral techniques rely on measurements made simultaneously by several
base stations. Accordingly, this is closely related to the network-based classifica-
tion. Unilateral means that the terminal performs measurements. Depending on
whether the evaluation is executed single-handed or after feedback signaling to
the network, this approach corresponds to the terminal-based or terminal-
assisted classification. Bilateral techniques finally apply autonomous measure-
ments for which either the terminal measures signals from a single base station
or one base station measures signals from single terminals.

4.2.2 Physical & Symbolic Localization
The result of localization is not necessarily composed of geometric or physical
information such as longitude, latitude and altitude, see Annex B. Instead, loca-
tion data is sometimes provided from a higher-level point of view also referred
to as symbolic localization. The applied basic principle here usually is ‘prox-
imity’ (see Section 4.2). Provisioning of symbolic information thus takes place
on a more abstract basis including location statements like ‘in the office’ or
‘close to an object’. Possible application areas are automatic information sys-
tems as installed in museums [192]. By indicating proximity to an object of in-
terest, respective systems automatically download an audio stream with detailed
information. The adjustable trigger zone thereby corresponds to the localization accuracy. Independent of the user’s position within the trigger zone, the same information is conveyed.

4.2.3 Absolute & Relative Localization

Absolute localization systems determine the current position regardless of previous positions, whereby a commonly known reference system is applied. For example, all GPS receivers use coordinates due to the 1984 revision of the World Geodetic System (WGS 84, [152]). To derive up-to-date position information, it is not necessary to record, request or provide any information from the past. Thus, two devices located at the same position will display the same coordinates regardless of their previous movement or switch-on time. From this point of view, absolute localization is a memory-free positioning technique.

In a system being based on relative position determination, each entity can define its own points of reference. E.g., with the localization of avalanche victims that carry a transmitter, the signal of the buried person is indicated to each rescue team with respect to its own location. Such, there is no necessity for a commonly agreed reference system making the positioning process autonomous. It is even possible to define self-contained reference points, which means that positions are recorded and used for future orientation. In this case, relative localization has the task to detect incremental deviants from the self-defined earlier reference points. In this way, it is e.g., possible to find back to a starting point when hiking or doing aquatic sports. From this point of view, relative localization is a memory-based positioning technique. However, the absolute location of a point can always be derived, e.g., by means of triangulation/trilateration, if the absolute positions of one of the reference points is known.

4.2.4 Self- & Remote Localization

Self-localization is a clear property of the terminal-based localization principle as presented above. With self-locating systems, the computation of the position is taken over by the located object itself. If localization is performed based on system inherent beacon reception, no additional explicit signaling becomes necessary. Further, self-localization is also a characteristic within the classification of the foreign system based/assisted positioning principle. For time critical applications like car navigation, it might be preferable to rely on self-derived positioning information representing always the latest whereabouts. In addition, data
security is given in the sense that no network device except the locating entity is aware of the respective position. Unless the object releases this information, concerns with respect to misuse as shortly addressed in Section 4.1 become obsolete. Disadvantages, in terms of increased terminal complexity have already been discussed for the terminal-based localization principle.

In remote-locating systems, the position computation is done centrally, i.e., in the network. Thus, remote-localization is a clear property of the network-based localization principle. Support by objects to be located is not necessary for the positioning process, which substantially reduces their memory requirements and needs for arithmetic performance. However, since usually a number of base stations is involved in the localization process of a single mobile, backbone traffic due to coordination and reporting increases. Further, safety and data security related questions are due to the sole objective of the network operators. Problems may arise if the deployment density is too small so that a mobile’s signal is only caught by one or two base stations. In addition, idle terminals cannot be tracked without further actions.

4.3 Cellular Localization

To determine a specific position, different localization methods may be applied making use of signals either of a cellular system itself or of complementary other systems. In the following, different metrics and methods with respect to localization in cellular networks will be discussed. The focus is on the applicability of self-contained localization of mobile radio networks, also referred to as Cellular Localization.

4.3.1 Cell Id

The most basic wireless location technology is given by the radio network setup itself. Modern mobile radio networks are composed of a cellular structure for higher spectral efficiency, allowing frequencies to be reused after a predetermined reuse distance [157]. Each base station periodically broadcasts important system information including a unique Cell Identifier (Cell Id). By evaluation of the Cell Id, latitude/longitude of the base station is taken as the mobile’s location. This means that Cell Id based localization can take place at the granularity (accuracy) of the actual cell size, see Figure 4.2, which can differ between some
4.3. Cellular Localization

Hundreds meters in dense urban areas up to 30 km in flat rural terrain. Obviously, further improvements can be achieved in case of cell sectorization. Localization based on the Cell Id is a suitable procedure for highly congested areas (urban areas) or networks with restricted bandwidth since no calculation and almost no (additional) signaling is required. Cell Id based positioning is fast and since it is an inherent property of all cellular systems, it can be applied with legacy mobile devices. The method is also denoted in literature as *Cell of Origin* (CoO) or *Cell Global Identity* (CGI).

![Figure 4.2: Localization based on Cell Identification](image)

Implementation of Cell Id based positioning may be carried out as terminal-based or network-based positioning (cp. Section 4.2.1). In the case of terminal-based implementation, the mobile needs to map respective Cell Ids to location information to derive absolute coordinates. For this, terminals either access internal information stored e.g., on the SIM card, or position information is gathered from control channels being continuously transmitted by the base station together with the Cell Id. An example for the latter case is the German operator O2 that conveys position information in Gauss-Krueger-format, see Annex B.4. Being a bilateral location principle (see Section 4.2.1), Cell Id positioning may also be realized as a network-based solution. Since the network is aware of a terminal’s current position due to entries in the Home Location Register, localization can take place without further signaling. The achieved accuracy thereby depends on the operation mode. If the terminal is in idle mode, accuracy corresponds to the size of the *Location Area* (LA) that usually comprises several cells. During ongoing communication or shortly after location update, accuracy corresponds to the size of the serving cell or sector.
4.3.2 Signal Strength

By using the signal strength as a metric for the distance and assuming free-space propagation between a mobile and a base station, the position can be estimated. In a two-dimensional environment, each venue is determined by its distance from three different points as pictured in Figure 4.3. Using omnidirectional antennas, the signal level contours have the shape of circles and the intersection of these curves is the sought position.

However, actual propagation is far away from free-space conditions, especially in urban areas. In addition, measurement accuracy suffers from fast fading and shadowing effects. Although the effects of fast fading can be smoothed by averaging and interpolation, this is not applicable for compensating the consequences of shadowing. Even the employment of adapted propagation models is a limited improvement. Thus, the variations in antenna orientation and local shadowing conditions around the terminal are seen as random errors in distance estimates and consequently in position estimation. Furthermore, location accuracy depends on adequateness of the propagation model as well as the number of available measurements [174].

Despite these dependencies, positioning based on Signal Strength is potentially more accurate than Cell Id based localization. Applying trilateration firstly allows for rough estimation of the relative position within a cell. Secondly, the incorporation of distances to other base stations further improves accuracy. Worst-case granularities of Signal Strength based positioning such correspond to the degree of cell overlapping.

![Figure 4.3: Positioning based on signal strength](image)

According to Section 4.2.1, the Signal Strength method is a unilateral technique that can be implemented either terminal-based or terminal-assisted. Similar to
4.3. Cellular Localization

Cell Id positioning, the terminal-based implementation relies on additional information (e.g., BS coordinates provided in beacon control channels) to determine the own absolute position. For the terminal-assisted realization, devices need to provide measurement feedback to the network that subsequently takes over trilateration calculation. However, this is not a problem since feedback signaling, e.g., in the context of power control, is already specified and applied in current cellular networks anyway.

In summary, Signal Strength based positioning is an easy and low-cost method that considers legacy terminals to enhance Cell Id based positioning. In fact, both methods usually are applied jointly.

4.3.3 Time-based Algorithms

A couple of algorithms rely on timing information to derive position information, whereby both, absolute and differential time stamps can be exploited. In a fully synchronized network, which means that the base stations as well as the terminals run synchronously, three absolute time stamps, used as an indirect method of calculating distances, are necessary for triangulation based 2D positioning. Exploitation of absolute times is characteristic for so-called *Time of Arrival* (TOA) positioning techniques.

In non-synchronized networks, such as GSM or UMTS-FDD, TOA techniques can only be used in a differential manner, for which the term *Time Difference of Arrival* (TDOA) is applied. However, the different base stations need a common time reference even in this case. Already a small timing discrepancy at either the transmitting or the receiving side causes a major error in the distance estimate. Table 4.2 exemplarily points out the impact of bit/chip duration and position estimation for GSM and UMTS. Applying one sample per chip/bit, the nominal rate of each system results in timing resolutions of $T_{\text{GSM}} = 3.69 \mu s$ and $T_{\text{UMTS}} = 0.26 \mu s$, respectively. The corresponding propagation distances are $D_{\text{GSM}} = 1108$ m and $D_{\text{UMTS}} = 78$ m. Four times oversampling as often performed by the receiver [190] results in decreased distances of $D_{\text{GSM,4samp}} = 277$ m and $D_{\text{UMTS,4samp}} = 19.5$ m.

Further enhancements with respect to accuracy are achieved by introduction of additional network elements, so called *Location Measurement Units* (LMUs). LMUs are fixed receivers at well-known positions. They can communicate error information to be considered within the final position calculation.
Table 4.2: Exemplary bit/chip durations and impact on position estimation

<table>
<thead>
<tr>
<th>System</th>
<th>chip/bit rate</th>
<th>bit/chip duration</th>
<th>propagation distance</th>
<th>Propagation distance (4 times oversampling)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>270.8 kbps</td>
<td>3.69 μs</td>
<td>1108 m</td>
<td>277 m</td>
</tr>
<tr>
<td>UMTS</td>
<td>3.840 Mcps</td>
<td>0.26 μs</td>
<td>78 m</td>
<td>19.5 m</td>
</tr>
</tbody>
</table>

In general, Time (Difference) of Arrival techniques are available in uplink as well as in downlink direction.

*Network based* T(D)OA on the uplink requires at least three base stations taking measurements of one single terminal. Potential drawbacks include capacity problems due to the multilateral measurement principle, high challenges with respect to synchronous operation of base stations and the fact that the mobile’s signal must be strong enough or the density of the BSs/LMUs high enough to reach three different base stations. The advantage is that due to the network-based implementation, uplink T(D)OA supports legacy phones. As such, it was taken up into GSM/UMTS standardization [178] as a candidate E911 solution.

*Terminal based* T(D)OA on the downlink requires a single MT to observe time (difference) arrivals from several BSs. Clock differences of the BSs can be solved by support of reference receivers such as LMUs that continuously measure observed time differences. This unilateral approach is much simpler and cheaper than synchronization of BS transmissions; however, it requires additional capabilities by the mobile.

### 4.3.3.1 Time of Arrival (TOA)

Time of Arrival is a technology that uses absolute time stamps at the receiver. For this, the transmitting stations need to adopt a high degree of synchronization. Figure 4.4 depicts a simplified two-dimensional view of this principle. A TOA system determines the position based on the intersection of the distance (or range) circles. Distances are calculated by multiplying the time-of-flight with the speed of light. Time-of-flight information thereby is derived from adjusting transmission time information encoded in the actual signal with local timers. Three range measurements determine a unique position. Geometric accuracy is the highest within the triangle formed by the centers of the three circles. It
gradually decreases when moving away from the triangle [178]. In general, accuracy is directly dependent on the nominal system rate with its resulting timing resolution and propagation distance as well as the applied sampling rate in the receiver.

![Figure 4.4: TOA positioning in synchronized networks](image)

A well-known system that applies TOA based localization is the Global Positioning System (GPS), see Section 4.4.1. Due to very precise timing, accuracies of some few meters are possible. In fact, the voluntary deterioration of GPS accuracy, called Selective Availability (SA), as performed by the US until May 2000, was based on artificially introduced time fluctuations.

### 4.3.3.2 Time Difference of Arrival (TDOA)

In contrast to hard-wired base stations, mobiles usually cannot synchronize accurately enough to assess directly the signal propagation delay. A possible solution to overcome the synchronization problem is to exploit differences in the signal propagation delay of several base stations rather than evaluation of absolute time stamps. Accordingly, this method is called Time Difference of Arrival (TDOA). With a minimum of three base stations receiving a signal from a terminal, triangulation is becomes possible. The differences in time delays of the signals, respectively the different distances to the base stations, are expressed by
\begin{align*}
\Delta D_{i,j} &= c^* \tau_{ij} = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - \sqrt{(x_j - x_0)^2 + (y_j - y_0)^2}, \\
\Delta D_{i,k} &= c^* \tau_{ik} = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - \sqrt{(x_k - x_0)^2 + (y_k - y_0)^2}.
\end{align*}

(4.1)

(4.2)

With \( c \) denoting speed of light and \( \tau_{ij} \) representing the observed time difference between the signals of base stations \( i \) and \( j \) as measured by the mobile, \( \Delta D_{i,j} \) denotes the distance difference of the terminal at position \((x_0, y_0)\) to one base station at position \((x_i, y_i)\) and another base station at position \((x_j, y_j)\). The same applies for \( \Delta D_{i,k} \). Hence, each of the equations (4.1) and (4.2) describes lines of constant distance differences \( \Delta D_{i,j} \) (\( \Delta D_{i,k} \)). Mathematically this corresponds to two hyperbolas as shown in Figure 4.5. A set of at least two equations involving at least three different base station coordinate pairs is required to solve for the two unknowns \( x_0, y_0 \). For additional altitude information, a third equation of this type, and thus a fourth independent BS site is required.

Figure 4.5: TDOA resulting in hyperbolic lines of constant differences

Application of TDOA positioning is one of the most popular methods within cellular localization. Within GSM, it is referred to as Enhanced Observed Time Differences (E-OTD) while UMTS specifies Observed Time Difference of Arrival (OTDA), respectively.

Another TDOA positioning technique, Advanced Forward Link Trilateration (A-FLT), has been standardized by Telecommunications Industry Association’s TR-45.5 as IS-801-1 and was taken over by 3GPP2 [180]. A-FLT is to be ap-
plied within cdmaOne and cdma2000. Unlike GSM and W-CDMA, these are inherently synchronous in their operation making measurements of time differences much easier. Distance based lateration is performed by exploiting the time difference (phase delay) between CDMA pilot signal pairs.

4.3.3.3 Timing Advance (TA)

Time based systems applying TDD schemes such as UTRA TDD need to adjust transmission with a high degree of accuracy. Depending on a system’s time resolution and the distance between transmitting and receiving station, the signal’s propagation delay cannot be ignored anymore. To allow for synchronous reception at the BS, the actual transmission point of time needs to be rescheduled to an earlier date, referred to as Timing Advance (TA).

Respective values for TA are determined by the network based on previous transmissions of the mobile. The terminal hereafter is briefed to schedule its transmission accordingly. The TA parameter therefore is known to both, the network and the terminal, and may be used as indirect measure of distances.

Depending on the time resolution and jitter, the area addressed by TA localization corresponds to a radial segment of a circle, as shown in Figure 4.6. If sectorization is applied, the addressed area may be narrowed down further.

![Figure 4.6: Addressed area by TA localization](image)
4.3.4 Angle of Arrival

*Angle of Arrival (AoA)* is a localization method that exploits the incident angle of arriving signals. A minimum of two different base stations, each equipped with an antenna array, suffices in order to apply AoA positioning, see Figure 4.7. Hence, AoA is a network-based technique applicable with all legacy terminals. Though installing and aligning antenna arrays on base stations can be a sensitive and costly process, it can be assumed that future installations will be equipped respectively for other purposes anyway, e.g., in order to support schemes such as beamforming for *Space Division Multiple Access (SDMA)*.

![Figure 4.7: AoA positioning based on incident angle](image)

A drawback is that AoA positioning suffers from decreasing accuracy for increasing distances. In addition, it requires line of sight propagation and is very sensitive for multipath signals. These are reasons for which AoA positioning is hard to realize in dense urban areas.

4.3.5 Database Correlation/ Fingerprints/ Pattern Recognition

This localization method is based on street modeling according to an operator's area prediction data and comparison with reported data. Position estimation initially might not be as precise as for some other (satellite based) methods, but being based on evaluation of existing data in the network, it can be used with legacy devices at low integration costs for operators.

The *Database Correlation Method (DCM)* [174] is a general method feasible for all kinds of cellular networks. The basic idea of DCM is that each object in a scenario has its specific influence on radio signal propagation. Superposition of all propagation paths results in a unique pattern that is specific to a given loca-
4.3. Cellular Localization

This fingerprint is compared with stored position-patterns from a database to find the most probable location. A possible fingerprint could be the pattern of signal echoes due to multipath propagation.

Major challenge for DCM is the creation and maintenance of the database. It must be trained for every new base station and changes in the environment since e.g., new buildings. For proper positioning, the resolution of the stored fingerprints must be adapted (it can differ between rural and urban areas). The number of measurement entries in the database determines its complexity and the potential localization accuracy. Nevertheless, this is the only technique that beneficially takes into account the properties and influences of the environment.

While DCM mainly addresses localization of non-moving users, pattern recognition further exploits changing fingerprints arising from roaming users. A pattern recognition technique based on Hidden Markov Models (HMMs) has been proposed by Kennemann in [181]. Further improvements are possible, if respective HMMs are trained with prediction data to model the strength of the received signals for particular areas. The use of HMMs enables street modeling and the construction of repositories for single street elements. The operator's prediction area data is used for training of HMMs by considering an assumed typical velocity distribution of the vehicles [182].

4.3.6 Hybrid Methods

Application of hybrid methods comprises the combination of two or more techniques to improve localization accuracy and precision. Hybrid methods perform in a way that strengths of the one technique compensate for the weaknesses of the other. Optimization efforts can be directed towards more reliable and/or more robust positioning. For hybrid localization it can be distinguished between a combination of

- cellular methods and
- cellular and non-cellular methods.

In the following, some examples for combining the previously presented cellular methods are discussed. Integration with non-cellular positioning techniques however, such as Assisted-GPS, will be described later in Section 4.4, in the context of satellite based positioning.
Enhanced Cell Id is a mechanism that combines Cell Id with one or more additional technologies to increase accuracy. In GSM networks, Cell Id is combined with Timing Advance and in W-CDMA networks, Cell Id is combined with exploitation of Round-Trip-Time. Measurements in the field for urban and suburban environments as exemplarily shown in Table 4.3 have been undertaken by Nokia and the finish operator Radiolinja [174]. For the urban environment, exploitation of Signal Strength in addition to Cell Id and Timing Advance gives results that are more accurate. In the suburban environment, however, using Signal Strength together with Cell Id and TA positioning is even counterproductive (Precision 67 %: 415 m → 448 m, precision 95 %: 844 m → 917 m).

Table 4.3: Accuracy for different precisions in (sub-)urban environments

<table>
<thead>
<tr>
<th>method</th>
<th>urban</th>
<th>suburban</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>67%</td>
<td>95%</td>
</tr>
<tr>
<td>CI</td>
<td>328 m</td>
<td>603 m</td>
</tr>
<tr>
<td>CI+TA</td>
<td>283 m</td>
<td>554 m</td>
</tr>
<tr>
<td>CI+TA+Signal Strength</td>
<td>207 m</td>
<td>429 m</td>
</tr>
</tbody>
</table>

increasing precision      increasing precision
increasing accuracy       increasing accuracy

4.4 Satellite Localization

While the focus in this thesis is on mobile radio aspects including cellular location techniques, satellite based positioning cannot be disregarded when addressing positioning. On the one hand, it is an important field with global scope; on the other hand, system integration as an inherent aspect of mobile radio B3G will not only provide means for interworking of different cellular technologies. Instead, allied techniques will be assimilated emerging in new services. Hybrid positioning techniques, such as Assisted-GPS that combines Global Positioning System (GPS) information and cellular information, will play key role in this development.
Global Navigation Satellite System (GNSS) is the general term for a satellite based positioning system. In the vernacular, these systems often are subsumed as Global Positioning System (GPS), though this notation depicts only the US-American approach. There are others such as the Russian Global Navigations-Satellite-System (GLONASS) or the European Galileo. However, the underlying basic principle applied for satellite-based positioning is always the same: Signal propagation delay from four or more satellites is evaluated to compute the current position.

The notation GNSS-1 is used to address projects dealing with improved performance of the existing military systems GPS and GLONASS in order to allow for civil application. Ground-based transmitter and geostationary satellites are deployed to offer improved quality of service to the user. Representatives of GNSS-1 systems are the European Geostationary Navigation Overlay Service (EGNOS), the US-American Wide Area Augmentation System (WAAS) and the Japanese Multifunctional Transport Satellite System Space-based Augmentation System (MSAS).

While GPS and GLONASS together with their augmentations stand for first generation satellite systems, the second generation, GNSS-2, is on its way. One representative here is the European Galileo project, which is expected to be up and running from 2008. Unlike GNSS-1 systems, which originate from military motives, GNSS-2 systems put the focus on civil services such as navigation support and emergency assistance. A major requirement for GNSS-2 systems thereby is their omnipresent availability with improved accuracy, velocity indication and data integrity. This shall qualify GNSS-2 systems to be used with safety critical applications, too.

4.4.1 Global Positioning System

The Global Positioning System (GPS) [183] is a satellite-based navigation and positioning system operated by the United States Department of Defense (DoD). The official name is NAVSTAR – GPS that is an abbreviation for Navigational Satellite Timing and Ranging - Global Positioning System; Sometimes, NAVSTAR is also used as short version for Navigation System using Timing and Ranging. In everyday usage, the system usually is referred to as GPS only.

The first GPS satellite was launched in 1978. Initial Operation Capability (IOC) was achieved in December 1993. At that time, 24 Satellites were prepared for
4. Localization Techniques & Principles

operation allowing for *Standard Positioning Service* (SPS) with target accuracies of about 100 m (95% reliability). *Full Operational Capability* (FOC), including *Precise Positioning Service* (PSS) with target accuracies of 22 m and 95% reliability, was announced in April 1995. Official launch of GPS dates from 17. July 1995.

GPS satellites orbit the earth every 12 hours at an altitude of approximately 20,200 km. Each satellite contains several high-precision atomic clocks and constantly transmits radio signals using a unique identity code. The GPS localization principle is based on Time of Arrival measurements (see Section 4.3.3). Satellites transmit two low power radio signals, designated L1 and L2. Civilian GPS uses the L1 frequency of 1575.42 MHz in the UHF band to transmit a spread spectrum signal including three different kind of information - a *pseudorandom code*, *almanac data* and *ephemeris data*. The pseudorandom code is used to identify the transmitting satellite. The almanac data tells the GPS receiver where each GPS satellite should be at any time throughout the day. Ephemeris data, finally, is essential for actual positioning since it contains important information about the status of the satellite (healthy or unhealthy), current date and time.

![Figure 4.8: GPS positioning based on trilateration](image)

Each GPS receiver disposes of a highly precise clock needed to measure the time delay between different satellite signals. On receiving at least three satellites,
4.4. Satellite Localization

Trilateration is used to estimate the receiver's location on a 2D plane. For 3D positioning, four reference points are needed, respectively. The time delay of each signal describes a sphere around the satellite, see Figure 4.8. The intersection of three spheres gives two points, one of which represents coordinates of the receiver’s latitude, longitude and altitude, the other one indicates a nonsensical position in space. The fourth reception signal is needed to compensate synchronization errors.

GPS is a worldwide operating system. To exclude non-authorized users (military opponents) from benefiting from precise positioning, Selective Availability (SA) was introduced to deteriorate artificially accuracy. The principle of SA is to introduce minor fluctuations within ephemeris data, e.g., sporadic time jitter. Being based on T(D)OA, this dramatically reduces the resulting accuracy. Since May 2000, SA is disabled allowing for high accurate positioning for civil applications, too, which was a precondition for the increasing success of car navigation and outdoor positioning in the recent years. When SA was still enabled, positioning was limited to approximately 100 m on average. Today’s GPS receivers are accurate to within 15 meters [196]. Satellite-based augmentation systems such as EGNOS, WAAS, and MSAS further decrease the total error to 3 - 5 m, revising clock errors, orbit discrepancies, and ionospheric effects. Similar improvements are possible for non-satellite based augmentation systems, e.g. Differential GPS (DGPS) or Assisted-GPS (A-GPS) as discussed in the next subsection.

In general, GPS accuracy depends on a set of factors such as the number of visible satellites, the receiver's movement or dominant atmospheric conditions see Table 4.4, whereby the given values may vary due to fluctuations [197]. Further effects that arise from theory of relativity due to gravitation and motion, have been inherently considered in the GPS design and do not play a significant role.

The substantial advantage of GPS is small personal costs for the end-user compared to the global system availability. A drawback of GPS is liability to multipath interference and its necessity to be in line of sight to at least 3 satellites for 2D localization and 4 satellites for 3D localization, respectively. While this is already hard to achieve in urban areas between tall buildings, this is almost impossible indoors.
Table 4.4: Major GPS Error Sources

<table>
<thead>
<tr>
<th>Impact</th>
<th>Discrepancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ionospheric disruptions</td>
<td>± 5-7 m</td>
</tr>
<tr>
<td>orbit discrepancies</td>
<td>± 2.5 m</td>
</tr>
<tr>
<td>clock errors</td>
<td>± 2 m</td>
</tr>
<tr>
<td>multipath propagation</td>
<td>± 0.01 - 10 m</td>
</tr>
<tr>
<td>tropospheric disruptions</td>
<td>± 0.2 - 0.5 m</td>
</tr>
<tr>
<td>miscounts and rounding errors</td>
<td>± 1 m</td>
</tr>
</tbody>
</table>

4.4.1.1 Differential-GPS

The Differential Global Positioning System (DGPS) allows for increased GPS accuracy by providing specific correction data. Fixed ground stations at well-known positions are used to determine discrepancies arising from position estimation based on satellite signals. Differential correction data is calculated and provided to GPS receivers, referred to as *Rovers*. DGPS was particularly useful when GPS was still degraded by Selective Availability resulting in improved accuracies of about 5–10 meters. Nowadays, even better resolutions are possible. The achievable accuracy thereby depends on the distance of the reference ground station to the Rover and the applied correction data. Three different methods are used:

- The simplest method is to convey sole position errors as determined by the reference station. The Rover applies this information to perform positioning corrections. A drawback of this method is that it only works in close distance to the reference station where the Rover is able to evaluate the same satellites as the reference station.
- Another method relies on calculating errors for the distances to the satellites (Pseudo range-correction). The advantage is that the Rover benefits by such information even if the subset of received satellites differs. Accuracies of less than 1 m are possible.
- The most reliable differential technique evaluates phase measurements of satellite signals (*Real-Time Kinematic*, RTK). Based on RTK, accuracies of ± 1 to ± 10 mm per km distance to the reference station are possible.
Main application area for DGPS according to the first two methods is navigation support while RTK accuracies are needed for geodetic checkups. The basic DGPS principle is illustrated by Figure 4.9. Transmission of DGPS correction data usually happens by VHF, medium wave or long wave radio transmission. By means of NTRIP (Networked Transport of RTCM via Internet Protocol), DGPS correction data is also broadcasted via the Internet. Since errors resulting from satellite signals vary rather slowly, DGPS information provisioning is not time-critical. Depending on the use case, DGPS can be applied in real-time directly in the field or when post-processing data in the office.

![Figure 4.9: Terrestrial DGPS principle](image)

### 4.4.1.2 Assisted-GPS

Satellite based positioning with GPS originally was developed for continuous outdoor positioning. Due to high accuracies, it is also interesting to be applied with mobile phones to serve as enabling technique for location based services. Problems of standalone GPS comprise:

- Long sensor start-up time
  - *Time-To-First-Fix* (TTFF) for standalone GPS usually is in between 30 - 60 s. For worst case scenarios, TTFF can rise up to more than 10 minutes [189]
• Weak satellite signal strength indoors and in urban environments
• High power consumption by the GPS receiver.

Assisted-GPS (A-GPS), or *Wireless Assisted-GPS* (WAGPS) as it is sometimes called when talking about A-GPS application for mobile radio, partly overcomes these problems. The mobile radio system thereby is used to provide further assistant information. Conventional GPS receivers perform two tasks: a) Pinpointing of signal arrival times and b) decoding of conveyed data.

A-GPS employs additional reference stations, usually in *Line of Sight* (LoS) to satellites. The reference stations take over most of the decoding tasks so that the supported GPS end-device may focus on signal arrival times. Hence, rather than detection and decoding of signals, simple detection is sufficient that allows operation at signal thresholds being reduced by 30 dB [188]. This increases the possibility to exploit A-GPS even indoors. In providing important assistant data via the mobile network, A-GPS releases the terminal from both, complex measurement actions and signal postprocessing. Reducing the search window of the code phase and the frequency space, the TTFF start-up time is expected to decrease to a few seconds only [189], e.g., knowledge of the satellite Doppler frequency mitigates the necessity to scan the entire frequency band. In addition, the terminal’s rough position is known due to the Cell Id (see Section 4.3.1). Hence, the mobile network can derive possible GPS satellites in reception range and signal their availability to the mobile. Since GPS applies CDMA with a specific code for each satellite, the number of necessary correlation steps within the mobile can drastically be reduced.

Applying A-GPS together with cellular location techniques in a hybrid manner allows the strengths of the one technique to compensate for the weaknesses of the other. Examples for hybrid positioning are Cell Id/A-GPS or E-OTD/A-GPS. According to [199], tight coupling of e.g., E-OTD/A-GPS dramatically increases service availability. Rather than being dependent on at least four GPS satellites, a combination of one satellite and two BTS’ or two satellites and one BTS is sufficient.
4.4.2 GLONASS

The *Global Navigation Satellite-System* (GLONASS) is a satellite navigation system that is operated by the Russian Space Forces. It serves as the Russian counterpart to the United States' GPS system.

Like GPS, the entire nominal GLONASS constellation comprises 24 satellites, 21 operating and three on-orbit 'spares' placed in three orbital planes. The first three test satellites were placed in orbit in October 1982 with the first operational satellites entering service in December 1983. The system was intended to be in operation by 1991 and it was announced to be operational on September 24, 1993. However, full operability was never reached. In 1998, up to 15 satellites orbited earth while their number hereafter decreased due to short lifetimes of only three years. Due to the economic situation in Russia, there were only eight satellites in operation in April 2002, rendering it almost useless for navigation. With improving economic situation, 11 satellites were in operation by March 2004. Following a joint venture with the Indian Government, it is proposed to have the system fully functional again by 2007.

GLONASS satellites orbit Earth at an altitude of 19,100 km being slightly lower than that of the GPS satellites with 20,200 km. The spacing of the satellites is arranged so that a minimum of five satellites are in view at any given time. At peak efficiency, simultaneous reception of four satellites offered a standard positioning and timing service giving horizontal positioning accuracy of 55 m and vertical accuracy of 70 meters, respectively. Velocity vector measuring was possible within 15 cm/s and timing within 1 μs. More accurate positioning was available for Russian military use.

4.4.3 Galileo

The Galileo positioning system [200] is a civil satellite navigation system, intended as a European alternative to the military-controlled United States Global Positioning System (GPS). It is designed to be independent but compatible with GPS. Due to enhanced properties such as omnipresent availability (≥ 99.8 %) and integrity, it is referred to as second generation Global Navigation Satellite System (GNSS-2), cp. Section 4.4.

A key driver for Galileo is the cognition that there is no alternative system to GPS to be used for civil applications. In addition, GPS accuracy is subject to US military administration that claims the right to decrease artificially accuracy any-
time and anywhere when considered necessary. Due political but also technolog-
ical reasons, European Union member states decided in 2003 that it is impor-
tant to have an own independent satellite-based positioning and timing infra-
structure to demonstrate an end to reliance on United States technologies. In ad-
dition, economical reasons play an important role: On the one hand, usage of
GPS signals is free for the end user, but on the other hand, all orders are given to
American companies that also hold licenses in producing end-terminals.

Technically, Galileo is relies on ground stations and 30 satellites (27 + 3 substi-
tutes) that orbit earth in 24,000 km. The first three satellites shall be launched
until 2006 and full operation is expected in 2008.

Five different services will be offered by Galileo:

- **Open Service (OS):** Public available, free of charge, accuracy of about
  four meters;

- **Commercial Service (CS):** To be paid for, accuracy less than one meter
  (in the range of cm if applied with augmentation systems);

- **Safety-of-Life-Service (SoL):** Used for safety critical fields, very robust
  and unforgeable signal;

- **Public Regulated Service (PRS):** Governmental applications, military
  use also possible;

- **Search And Rescue (SAR):** worldwide localization of casualties, simple
  two-way communication, e.g., “Assistance is on the way”.

### 4.5 Accuracy & Precision

So far, the most important (cellular) location techniques have been introduced.
In general, the aim of localization is to determine locations accurately and pre-
cisely. Having a look at positioning performance as shown in Table 4.3 respec-
tively at manufacturers' instructions of e.g., GPS devices, one will always find
statements on both, accuracy and precision, e.g.,:

1. “A receiver can give you a position accuracy of better than three meters
   95 percent of the time”, [196] (accuracy: 3 m, precision: 95 %).
2. Other assertions promise positioning granularities of 10 meters for ap-
   proximately 99 percent of measurements (accuracy: 10 m, precision:
   99 %).
Thus, accuracy as used here means the *granularity* with which objects may be located while precision means the *reliability* that a located object really resides within the accuracy range of the determined position. Synonyms used for ‘precision’ within literature comprise ‘reliability’, ‘integrity’ or ‘quantile’.

Figure 4.10a) provides an impression of different aspects related to accuracy and precision. If the target area is the hatched circle in the middle, the size of colored circle as well as its overlapping with the target area correspond to a respective couple of accuracy and precision. Increased accuracy is indicated by a decreased radius of the colored circle. Increased precision is registered, if the overlapping of green circle and target circle increases as well.

![Figure 4.10: Aspects of accuracy & precision and mutual interdependency](image)

However, while Figure 4.10 a) addresses different aspects expressed by accuracy and precision, it does not convey their interdependency. In fact, both, accuracy and precision are closely dependent on each other. Changing one parameter directly affects the performance of the other. If *one single* localization technique is applied, *increasing accuracy* is only possible for *decreasing precision* and vice versa. Measurement results presented previously in Table 4.3 prove this statement.

The interdependency of accuracy and precision shall be clarified with the help of see Figure 4.10 b). The abscissa (Δx) depicts a possible localization error (difference between the object’s real position and the position determined by the applied positioning technique) while the ordinate shows the corresponding prob-
ability of occurrence. In this example, it is assumed that the resulting error density of imprecise localization follows a Gaussian distribution.

Accuracy of localization increases if the resulting localization error $\Delta x$ decreases. In other words, increasing accuracy means a decreasing numerical value of location resolution, e.g., location resolution of 5 m instead of 10 m. Thus, positioning accuracy is inversely proportional to the localization error $\Delta x$.

The precision (also referred to as reliability) of localization corresponds to the integrated surface as hatched in Figure 4.10 b). Thus, if the target accuracy is increased, precision usually decreases. For practical application, this means on the one hand that a dedicated single positioning technique may allow for very high accuracies but obviously at the risk of entailing a higher number of samples that in fact are not inside the acquired accuracy range. On the other hand, if the reliability (= precision) that an acquired sample really resides in the determined area shall be increased, the demands on accuracy need to be less strict. Against this background, the initial manufacturers’ statements on accuracy and precision are to be checked again (decreasing accuracy: 3 m $\rightarrow$ 10 m, increasing precision: 95 % $\rightarrow$ 99 %).

To achieve a concise quantitative summary of accuracy and precision, actually these terms need to be considered including a remaining unsteadiness expressed by an error distribution incurred when locating objects [156]. Thus, the actual outcome of a positioning operation is rather a statistical distribution than a single spot. For this reason, the notation ‘position space’ is sometimes used in literature. Additional dependencies to be considered comprise the necessary density of infrastructural elements and their deployment. An encompassing characterization of positioning could be expressed like this: ‘Equidistant deployment of 10 WLAN access points in an exhibition hall with a floor space of 2500 square meters applying a localization principle X allows for positioning accuracies of 5 m with a precision equal to 95 % and error margins defined by a Gaussian distribution being centered at the object’s real position and having a standard deviation of 2 m’.

However, in most of the cases accuracy will be the most important criterion to judge whether a specific positioning techniques is to be applied (whereby an inherent minimum precision value is assumed, e.g., 67 %). Motion-capture installations for remote control or computer animations need to operate with resolutions down to few centimeters, car navigation is fine with accuracies in the order of meters and location area management as applied in cellular networks relies on
accuracies of several hundred meters up to some kilometers. Precision can be increased by increasing the number of samples whereby statistical runaways may be sorted out by further coupled mechanisms.

Within this thesis, measurement reports are combined with location information for further processing by a Hybrid Information System. The impact of different localization methods resulting in different positioning performances thereby needs to be considered. Rather than explicitly referring to a dedicated location technique, imprecise positioning will be modeled by applying respective values for accuracy and precision according to different (hybrid) location techniques. Modeling of location imprecision is presented in Section 6.1.1.

4.6 Summary

Within this chapter, characteristics and properties of localization have been presented. Position information generally is seen as enabler for Location Based Services (LBS). While LBS currently are not yet widely deployed, prognoses predict extraordinary potentials making it a possible killer application for next generation networking. One driver for this development is the US911 regulation that requires operators and manufacturers to work out solutions to support positioning for emergency aid. Similar aims are followed by the European initiative E112. Once the technological preconditions are fulfilled by a critical mass, launch of omnipresent LBS is expected.

Two positioning concepts, cellular-based and satellite-system based localization are applicable. Both entail advantages and disadvantages in specific environments. While some cellular-system based methods are easy to realize at few additional costs and with legacy mobile devices, accuracy is restricted to some hundred meters. If accuracy shall be increased, more effort is necessary, e.g., by introducing additional entities (LMUs) to the cellular network. Hence, if higher accuracy is required, satellite-based systems such as GPS provide better performances. Well-known drawbacks here comprise restricted availability indoors and in urban areas as well as additional hardware requirements in mobile devices.

Which solution finally will prevail, depends on the required accuracy for the aspired location based service and its deployment costs, both, in the core network part and the user-terminal. Meanwhile, hybrid solutions in terms of A-GPS are advancing, e.g., T-Mobile has executed large field trials with A-GPS solutions in the Czech Republic and Siemens announced IP-based A-GPS solutions to be on the market at the end of 2006 [198].
Some major properties of the most important localization methods have been summarized in Table 4.5. Accuracy usually applies precision values of 67%. If no percentage value is given, data is estimated based on existing techniques. The ‘Active’ column says if the mobile is involved in the position estimation or if this is completely done by the network and the base stations. Several of the techniques depend on the reception of at least three base stations. Hence, they are focused on urban or suburban areas. This property is shown in the 4th column. The ‘Standard’ column depicts whether the technique is already introduced in the specification or not. ‘Additional Signaling’ finally states if there is an information exchange necessary between user terminal and network.

**Table 4.5: Properties of positioning techniques**

<table>
<thead>
<tr>
<th>Positioning Technique</th>
<th>Accuracy(^{23})</th>
<th>Active</th>
<th>Area urban/suburban/rural</th>
<th>Standard</th>
<th>Additional Signaling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell Id</td>
<td>250 m-30 km (100%);</td>
<td>Network</td>
<td>imprecise</td>
<td>GSM/UMTS</td>
<td>NO</td>
</tr>
<tr>
<td>Signal Strength</td>
<td>200-448 m (67%)</td>
<td>Mobile</td>
<td>good/good/low 3 BSs required</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>ToA</td>
<td>50-200 m (67%)</td>
<td>Network</td>
<td>good/good/low 3 BSs required, Synch.</td>
<td>GSM</td>
<td>NO</td>
</tr>
<tr>
<td>E-OTD</td>
<td>50-125 m (67%)</td>
<td>Mobile</td>
<td>good/good/low 3 BSs required</td>
<td>GSM</td>
<td>YES</td>
</tr>
<tr>
<td>OTDOA</td>
<td>20-200 m (67%)</td>
<td>Mobile</td>
<td>moderate/moderate/low near-far problem, hearability</td>
<td>UMTS</td>
<td>NO</td>
</tr>
<tr>
<td>AoA</td>
<td>100-200 m; 45 m (67%);</td>
<td>Network</td>
<td>good/good/moderate 2 BSs required, LoS</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>DCM</td>
<td>44-74 m (67%)</td>
<td>Mobile</td>
<td>good/good/moderate 1 BS required, high effort</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>A-GPS</td>
<td>5-10 m (67%)</td>
<td>Mobile</td>
<td>moderate/good/good additional hardware</td>
<td>UMTS</td>
<td>YES</td>
</tr>
</tbody>
</table>

\(^{23}\) Accuracy information is compiled from various sources of literature. Being highly dependent on environmental conditions, these values shall be taken as exemplary only. Variations in live networks are possible.
CHAPTER 5

Hybrid Information System

Content

5.1 Motivation ......................................................................................... 140
5.2 Basic Principle................................................................................... 140
5.3 Overview ........................................................................................... 141
5.4 Data Administration .......................................................................... 146
5.5 Application Areas ............................................................................ 151
5.6 Realization Aspects: Mapping to 3/4G Architectures ....................... 153

Keywords: Hybrid Information System, Data Administration, Information Exchange, Reference Architectures

The following chapter introduces the basic concept of the Hybrid Information System (HIS) for the integration of heterogeneous networks and describes in more detail related logical entities. Focus thereby is put on feeding of HIS, internal data administration and data supply. In addition, it is pointed out how HIS data - once gathered - can be employed further. It is shown that the HIS approach has been adopted by leading IST-projects such as WINNER (cp. WINNER WP4, deliverables D4.3 [116] and D4.4 [117] ) making it a promising concept within future networking. Accordingly, realization aspects for the Hybrid Information System have been taken up in this work. In detail, HIS integration in the reference architectures of 3GPP Location Services, WLAN/3GPP Interworking and WINNER Logical Node Architecture are presented. An overview of related work concludes this chapter.

24 The initial idea for the Hybrid Information System has been developed by the author at the Chair of Communication Networks in the framework of industrie cooperation with Siemens AG. Patents on national [118] and international [119] level have been assigned. An overview on HIS has been published in [120].
5.1 Motivation

The widespread seen need for research with respect to system integration is an indicator for the challenges to be satisfied by next generation mobile communication. Rather than being reliant on one single wireless communication technology, integration and cooperation of complementary radio access networks, each optimized for specific requirements, will play a key role. Nonetheless, overlaps with respect to service support offered by each system are natural and necessary. Smooth and seamless service support across network boundaries is a sophisticated target to be realized.

To allow for appropriate network selection, respective decision algorithms are reliant on system information concerning general existence, current availability and offered QoS support of candidate systems. State-of-the-art information gathering is accomplished by means of self-conducted scanning. However, it will be shown that scanning entails a couple of drawbacks making it a suboptimal means for information gathering only.

The following chapter introduces a new concept, referred to as Hybrid Information System (HIS), which provides a platform for inter-system information exchange. Particular focus is put on the application of context information in terms of location. In addition to accomplishment of detrimental scanning impacts, HIS turns out to serve as enabling concept for supply of new services in the context of next generation networks.

5.2 Basic Principle

Every wireless communication system applies feedback information from its associated stations in order to optimize transmissions. This feedback information usually become manifest in Measurement Reports (MR) used to support e.g., power control or link adaptation algorithms. In addition, MRs taken by the network itself are available.

The basic idea of the Hybrid Information System is to associate measurements with position information and store them to a database. Based on this data, it is possible to provide mobile terminals with information about heterogeneous systems using the current communication link. A station hence may request link state information for a complementary system, mitigating the need for self-
conducted scanning. The requesting station’s current position, derived from self- or foreign localization, is used to match respective entries in the HIS database.

Rather than working on a stand-alone basis, *information transfer* is exactly what is promoted by the Hybrid Information System. Thereby it is to underline that the basic HIS approach does not introduce additional signaling overhead to the air interface due to *re-use of existing information* being available in the system anyway.

### 5.3 Overview

The basic idea behind the HIS approach is illustrated in Figure 5.1. Each system reports about its current state, i.e., link conditions and interference distribution. Together with a measurement report, the location of the reporting mobile MT A is registered (1). All data is stored in a database (2) so that a mobile MT B of another system willing to change may request\(^{25}\) this information. Matching attribute of the request is the current position of MT B. Depending on the new target system, MT B is supplied with state reports of the same system type (for horizontal handover, HHO) or of a vertical system (for VHO), cf. (3, 4, 5), and subsequently may perform the (V/H)HO, see (6).

#### 5.3.1 Feeding & Information Clients

While Figure 5.1 is meant to visualize the overall HIS concept, Figure 5.2 explains involved entities and their interaction. On the left side of the figure, one can see the so-called *Feeding Clients* of System A and B as well as the respective *Information Clients*.

The vertical separation between those clients indicates their logical separation and is not related to the actual geographic position during operation. Feeding clients are inherently all mobiles that transmit measurement reports to the fixed network. Mobiles may act as feeding client without even being aware of this task, e.g., terminals sending information about power control implicitly provide information on their link conditions to be exploited by HIS.

---

\(^{25}\) Intersystem information requests are not part of current (intra-)system protocols. The method introduced in this thesis opens up a new way of information exchange relying on legacy HO messages.
Information clients are terminals that somehow make use of the information provided by HIS. It is worth mentioning that HIS is not restricted to the control of heterogeneous systems, but may also be applied for performance enhancement of homogeneous systems. If the information is used e.g., to support HHO, feeding and information clients are associated with the same RAN. Nonetheless, the actual signal flow is realized via HIS that serves as logical connection point for both, horizontal and vertical information exchange.

### 5.3.2 Localization Units

The basic property of HIS is to map incoming measurement reports to specific locations. Therefore, it is important to support localization of the feeding clients. In principle, two localization approaches are possible: Either Feeding Clients perform self-localization, indicated by the two *Self Localization* boxes on the left side of Figure 5.2, or HIS acquires a feeding clients’ position by *Foreign Localization*, indicated by the respective box in HIS.
5.3.3 Service Control & Data Administration Units

Central elements of the Hybrid Information System are the two units for Service Control and Data Administration. The task of the service control unit is to administer incoming requests from information clients and to respond adequately with trigger or recommendations for HO. For this, the Service Control Unit implements dedicated calculation and decision entities. Depending on the purpose for which data shall be used, filtering and averaging of information in the time and/or space domain is performed, e.g. as usual for HHO in systems like GSM or UMTS.

The Data Administration Unit is responsible for acquisition and management of the entire HIS data set. This can be either pure location data provided by the Foreign Localization Unit, or a joint combination of measurement reports with affiliated position data as provided by any Feeding Client. It may further implement pre-filter functions to provide only a subset of its entire data set to the decision entity of the Service Control Unit.

![Diagram of Feeding, administration and supply of data within HIS](image)

**Figure 5.2: Feeding, administration and supply of data within HIS**
Depending on the level of integration, the Service Control Unit may not only take over passive and reactive operations like the respond to explicit information requests but also (pro-)active tasks. As an example, it can monitor and track movements of a respective station of system A and autonomously provide a trigger as soon as the station enters the coverage area of another (vertical) system B with better radio conditions or properties. Pro-active operation hence results in network controlled HO as introduced in Section 3.3.2.4.

Based on well founded and up-to-date HIS information, a new quality of the Always Best Connected (ABC) paradigm is aspired. In addition, the Service Control Unit disposes of interfaces to entities such as the Home Subscriber Server (HSS) or Radio Network Controller (RNC) allowing for incorporation of further aspects within the VHO decision-making process such as user preferences (from HSS) or allocated system capacity (from RNC). The integration of HIS into 3/4G system architectures is further discussed in Section 5.6.
5.3.4 Passive & active operation

In passive or reactive operation mode, HIS does not provide any triggers unless explicitly requested by a mobile terminal. The initial action hence is taken by the mobile asking for specific recommendations. Receiving a request, HIS takes into account the mobile's current position and determines available complementary radio access networks according to stored measurement reports from third party feeding clients. Hereafter, all information is forwarded to the station for further processing. Such, HIS releases the terminal from the necessity for self-conducted scanning and allows single transceiver stations to maintain the current connection though performing detection of complementary systems. All information is conveyed to the mobile terminal applying the originally active association.

The (pro-) active operation mode allows HIS to send autonomously recommendations to mobile terminals without prior request. Based either on a periodic schedule or event-triggered, e.g., due to reception of a new measurement report, HIS checks ongoing connections under its control and determines whether the ABC target is satisfied. An anticipated advantage of the active operation approach is that signaling overhead is likely to be reduced. Mobile terminals do not need to poll HIS for recommendations but get update information only when a positive vertical handover decision was taken. This holds particularly if network-based positioning is applied since terminals do not even need to provide their current position.

In accordance with Section 3.3.2.4 on handover control, passive operation can be classified as Mobile-Initiated HandOver (MIHO) while active operation of HIS belongs to the Network Initiated HandOver (NIHO) domain. Accordingly, the integration of the HIS concept in existing architectures is to be characterized as loose coupling for passive operation and tight coupling for active operation, respectively.
5.4 Data Administration

5.4.1 Feeding of the Hybrid Information System

HIS administers databases reflecting the current link conditions, e.g., interference situation, in each of its associated subsystems, see Figure 5.2. Assuming that localization predominantly takes place by the network (foreign localization), in principle there is no additional signaling between the mobiles (feeding clients) and the BS/AP necessary for maintaining HIS databases. The respective information should be available at the base station anyway, e.g., in the context of power control, link adaptation related signaling or number of automatic repeat requests.

5.4.2 Internal Data Processing

To allow for a reliable and smooth operation of HIS, incoming data from the feeding clients needs to be administered and stored. For this, a set of database servers is associated to the Service Control Unit in HIS, as shown in Figure 5.2. Their task is the reliable and fast storage and access to dedicated system information. Basic entries in the databases comprise a compound of measurement reports, positioning data and time stamps. By such, an internal representation of the link/interference condition within each associated radio system, a so-called link state map, is achieved.

5.4.2.1 Storage of HIS data

With the reception of new measurement reports, an update of the link state map is triggered. Accordingly, the map has a different set up at respective points of time (t₁, t₂, t₃, t₄, …) as it was indicated in Figure 5.2, resembling ‘salami’ slices. The minimal thickness of those slides is directly related to the inter-arrival times Δt of measurement reports. Besides for a time concerned description of maintained data, the ‘salami’ metaphor matches well in another sense: The granularity of the slices corresponds to the spatial resolution Δx and Δy, with which HIS may provide interference information. Spatial resolution is directly related to the penetration and position of feeding clients.
Data storage is possible by application of different internal data structures as shown in Figure 5.4. Measurement reports either are quantized both, in time and space domain (Approach A) before storage, or the database entries contain raw data (Approach B) meaning that a dedicated entry is written for each incoming report. Both approaches feature by different properties. While Approach A potentially results in less administration overhead and faster data access than Approach B, quantization introduces further errors (local and time fuzziness). Further pros and cons are:

<table>
<thead>
<tr>
<th>Approach A (quantization)</th>
<th>Approach B (storing raw data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Only one array of data per short-, mid-, and long-term data</td>
<td>+ Different algorithms can be applied anytime</td>
</tr>
<tr>
<td>- Different evaluations (e.g., memory depth) cannot be changed on demand</td>
<td>- Amount of stored data might be huge</td>
</tr>
</tbody>
</table>

Within this work, an implementation according to Approach B has been favored. Dedicated filters (such as the Decision Area, see Section 7.5.1) are used for data evaluation. Similarly, dedicated algorithms, e.g., averaging, considering time and space domain need to be applied if requests are made for positions with no entries or out-of-date entries.

The modular HIS approach allows for incorporation of further parameters into the database. Extended entries could consider properties such as velocity, moving direction, current service consumption and others. This is how personalized service provisioning as well as prediction techniques can be supported. Further examples for enhanced application of HIS data are given in Section 5.5.
5. Hybrid Information System

5.4.2.2 Short-, mid-, long-term data

An interesting point with respect to usability of HIS information is the use case, for which respective data shall be applied. Obviously, handover decision taking should not be based on out-of-date interference information. On the other hand, system engineering with respect to detection of areas with permanent poor coverage does not require knowledge of current fading figures. However, the concept of HIS accommodates both needs by distinguishing between short-term, mid-term and long-term data (see Figure 5.2).

**Short-term** data is meant to support real time requests from the information clients. As soon as feeding clients provide new measurement reports, the information is written without further filtering to the HIS database. Hence, short-term data reflects the latest entries in the database. While short-term data is not suited to cope with short-term fading (measurement intervals still are too long and some averaging is included as well), the life cycle of respective information is short enough to serve as decision basis for short-dated handover triggers, LA/PC support and the like. After a pre-defined time interval, short-term data needs to be deleted or classified as mid-term data.

**Mid-term** data is less time critical. It is based on short-term input but due to respective filtering and averaging, time selective fading effects are equalized. Nonetheless, mid-term data is of interest for ongoing communication since it serves as reference, in particular for predictable actions. Especially in combination with prediction and profiling, see Figure 5.2, mid-term data is useful for planned handover triggering, (joint) Radio Resource Management (RRM) or Connection Admission Control (CAC).

**Long-term** data addresses either permanent impacts or recurring events. The first could be determination of areas with ongoing insufficient link quality while the second applies to e.g., daily occurring network congestions during rush hours. Effects like cell breathing or sudden interference are eliminated. The period for long-term data is supposed to be longer than one day. Table 5.1 summarizes the basic properties of short-, mid- and long-term data.
### Table 5.1: Characteristic properties of short-, mid- and long-term data

<table>
<thead>
<tr>
<th>Short-term data</th>
<th>Mid-term data</th>
<th>Long-term data</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Support of ongoing handover execution</td>
<td>- based on short-term data</td>
<td>- based on mid-term data</td>
</tr>
<tr>
<td>- Decision basis for time critical controlling</td>
<td>- averaged/extracted from short-term data</td>
<td>- cell breathing excluded</td>
</tr>
<tr>
<td>- Fading (partly), shadowing and other propagation effects included</td>
<td>- quasi-static character</td>
<td>- Considers potential periodicities</td>
</tr>
<tr>
<td>- High variance over time</td>
<td>- short-term fading excluded</td>
<td>(e.g., regular rush hour)</td>
</tr>
<tr>
<td>- Short life cycle (&lt; seconds)</td>
<td>- cell breathing still included</td>
<td>- Used for network planning [121]</td>
</tr>
<tr>
<td></td>
<td>- shadowing included</td>
<td>(optimization, coverage detection, shadowed areas)</td>
</tr>
<tr>
<td></td>
<td>- Life cycle min - hours</td>
<td>- Life cycle &gt;= 1day</td>
</tr>
</tbody>
</table>

As explained, short-, mid- and long-term data are derived from different averaging and filtering of HIS data. The basic idea behind this is that different algorithms depend on different sets of data, all of which being supplied by HIS. To increase the coverage or adapt to different loads in a system, an algorithm that dynamically adjusts the down-tilt of base stations’ antennas may be employed. This algorithm can use the mid-term or long-term data as input to its calculations. To support algorithms like handover, link adaptation or power control, short-term or mid-term data is to be used.

The logical separation in short-, mid- and long-term data directly affects the complexity of the database. For the different types of data, three different filters are considered, see Figure 5.2. Due to high challenges with respect to Time To Respond (TTR) and memory, database queries concerning short-term data are expected to be much more challenging than respective long-term data inquiries. It is also possible to physically separate administration of short-, mid- and long-term data. As a basic rule, short-term data should be accessible by air-interface controlling entities as quickly as possible. A detailed discussion on physical mapping of HIS functionality to 3/4 G architectures is provided in Section 5.6. Apart from filtering of data in the time domain, additional filtering algorithms in the space domain will become necessary, e.g., if information is requested for positions for which no entry exists in the database. A possible solution for this is to rely on entries for positions having minimum Euclidean distance.
5.4.3 Data Supply

In general, two controlling schemes are possible: First, decisions such as handover control can be network based and second, decisions can be mobile based. The chosen approach corresponds to the way HIS is involved in information provisioning: HIS may either ‘work on request’ meaning that information is only provided after an explicit request was received (MIHO scenario) or HIS may play a more active part and provide information autonomously to the terminals (NIHO scenario). Even the realization of push services based on HIS information is thinkable.

An open question concerns data transfer from HIS to the end-user. While feeding of HIS happens without additional traffic, information provisioning needs explicit signals. Obviously, this is only necessary, if the mobile is in control. Network based controlling does not require noteworthy extra signaling. Anyway, if information needs to be provided to terminals, there are different options: One is to use resources of the current system. For this, existing broadcast channels could be enhanced to transmit neighboring-cell and foreign system related data. Obviously, the introduced overhead is a clear disadvantage of the enhanced broadcast solution. Therefore, the requested information could be transmitted in an in-band fashion, piggybacked with other data the MT is exchanging with its actual base station. In such a way, only a dedicated MT receives particular data.

5.4.4 Self-Healing property

An assumed drawback of the HIS concept is that the loading of HIS databases depends on the number and position of feeding clients. If namely only few feeding clients provide measurement reports, this has a direct impact on both, the spatial resolution and the time resolution of the maintained interference maps. However, concerning the long-term data this is of minor influence. The only difference is that the timeframe for the collection of data needs to be extended so that sufficient probes/measurements reports can be evaluated with statistical reliability. Concerning the mid- and short-term data whose intention is to support in-time decisions, a high number and timeliness of measurements from feeding client seems to be inevitable. Nonetheless, recalling the original intention of information requests by the clients opens up the self-healing property of the HIS concept:

Either, the target system is highly penetrated with feeding clients. This results in a proper and up-to-date interference map of the target system/area. Hence, a mo-
bible willing to handover gets a precise image of the target system and may estimate based on this input whether a handover is worthwhile or not. Alternatively, only a few feeding clients are available in the target system. In that case, HIS interference maps are rather fragmentary. However, fragmentary or non-complete link state maps entail information themselves: First, they indicate that the target system is not fully loaded and second they visualize for which positions reduced interference can be expected. In such a way, HIS information is helpful for both cases, high and low penetration, what is referred to as ‘self-healing property’ of HIS.

5.5 Application Areas

Once HIS databases have been initialized, resulting benefits are not only restricted to ongoing communication. Especially long-term data holds a high potential for further optimization tasks. In combination with profiling, personalization and prediction, conventional services are to be improved and new applications can be invented. The following subsections describe HIS application areas that will be further investigated within this thesis. However, there is much more potential that cannot be all addressed within this work. A short outlook in Annex A indicates further interesting application areas.

5.5.1 Handover triggering

The relevance of HIS for supporting vertical handover has already been described in Section 5.3 with the help of Figure 5.1. However, it is worth mentioning that HIS data may also be used for horizontal handover support as indicated in Figure 5.2, where feeding client and information client belong to the same (horizontal) system. Due to overlapping cell areas in conjunction with hysteresis, it is possible that two locally closely located terminals are subscribed to neighboring BS/AP. Instead of performing intra-system measurements, respective information may also be requested via HIS.

5.5.2 Network/Coverage optimization

Based on the long-term data evaluation as introduced in Section 5.4.2, it is possible to detect areas with permanent or recurrent link failures. Permanent problematic areas may refer from inconsistent or antiquated BS/AP installations. The latter may occur e.g., in development areas where the radio infrastructure has
been installed prior to the building of new houses. Recurrent link failures are evidence of periodic appearing incidents, such as rush hour or mass events. Exploitation of HIS data helps to determine affected areas and to set off dedicated counter measures.

5.5.3 Link Adaptation & Power Control
Link Adaptation (LA) and Power Control (PC) aim at transmitting data in a spectrally most efficient way by reducing interference as much as possible. However, usually the applied algorithms follow an iterative control loop meaning that actions are performed in a reactive manner as a response to incoming failure messages or measured bit error ratios. With the help of HIS, a more proactive adjustment of chosen LA and PC can be achieved. For example, if a terminal handovers to a new target system, it may directly start transmitting with an adequate PHY-Mode respectively transmission power since it can rely on measured BER from other terminals. By such, the swing-in period of the control loop can beneficially be decreased. For UMTS, support in the adaptation process of the outer loop power control is conceivable.

5.5.4 Adaptive Beaconing
All radio communication systems comprise information channels used to provide system information. Within IEEE 802.11, these information channels are referred to as beacons. Reception of beacons is of particular interest for terminals that want to associate with the AP. However, if there is no station being reliant on upcoming beacons, broadcast of system information results in signaling overhead.
Application of the Hybrid Information System with respect to adaptive beaconing presents itself from several points of view: First, beacon transmission may be scheduled according to specific needs, e.g., providing terminals with system information immediately before or straight after VHO execution. Second, directed beaconing applying beamforming allows for provisioning of system information to specific areas only.
Hence, adaptive beaconing comprises sophisticated control mechanisms in both, time and space domain. Both aspects will be investigated and discussed in the scope of this thesis.
5.6 Realization Aspects: Mapping to 3/4G Architectures

The previous section provided a high-level description of properties and services supported by the Hybrid Information System. Though the scope of this thesis is on radio aspects, the following description focuses on (core) network architectures to point out that HIS has a concrete realization touch with existing and currently developed system designs.

The actual HIS benefit is to bundle (upcoming) available features as specified among different 3GPP releases and within IEEE. Hence, the Hybrid Information System needs to be seen as a complex logical unit (distributed realization approach) rather than a single physical entity (centralized approach). This is inline with other specifications such as e.g., the IP Multimedia Subsystem (IMS) [179] that comprises different core network elements in order to provide IP multimedia services. However, a centralized ‘black box’ approach is possible as well. In this case, all data needs to be conveyed to HIS, but obviously at the cost of increased (core network) traffic. In addition, duplicate data administration is necessary, both, in the providing entity and in HIS.

Depending on the degree of integration in existing radio technologies one can distinguish two operation modes for the Hybrid Information System. An early step with rather loose integration would be to implement HIS in passive operation mode, which means that mobile terminals actively request information. No communication is initiated by HIS itself. In a second step, a tighter coupling between radio systems and HIS can be aimed at. HIS becomes part of the radio access network and actively proposes handover recommendations to associated mobile terminals.

5.6.1 Location Services Architecture of 3GPP

Starting with GSM Phase2+ Release 98, a description for the Location Services (LCS) feature on GSM was specified providing the support of mobile location services not being covered by standard GSM. In an initial stage 1 description [178], a generic flexible LCS architecture is introduced providing support for emergency services, value added services, and PLMN operator services. With Release 99, a new stage 1 description on LCS service aspects, TS22.071 [184], was compiled with enhancements to support both GSM and UTRAN to facilitate determination of the location of a mobile station.
While in principle all positioning methods should be considered, special support for dedicated techniques was specified in subsequent LCS stage 2 specifications dealing with technical realization aspects. While stage 1 is a more general description comprising one single specification valid for GSM and UTRAN, stage 2 is more specific. Localization methods being explicitly mentioned comprise **Time of Arrival (ToA)**, **Enhanced Observed Time Difference (E-OTD)** and GPS assisted positioning methods.

![Figure 5.5: LCS specification development and status](image)

The HIS concept is based on combined evaluation of location related measurement reports. This in turn means that databases need to be present to administer respective input data for both, location management and link status aggregation. The following section describes shortly the tasks of important network entities and explains their relation to the Hybrid Information System.

**5.6.1.1 General Location Registers**

An indispensable must for mobile radio networks is mobility management. In order to support ubiquitous reachability for roaming users dedicated databases, so called **location registers**, administer whereabouts of associated terminals. Location register functions are handled by four different entities:
Table 5.2: 3GPP specifications & reports with respect to Location Services

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS 02.71</td>
<td>Location Services (LCS); Stage 1</td>
</tr>
<tr>
<td>TS 03.71</td>
<td>Location Services (LCS); Functional description; Stage 2</td>
</tr>
<tr>
<td>TS 04.30</td>
<td>Location Services (LCS); Supplementary service operations; Stage 3</td>
</tr>
<tr>
<td>TS 04.35</td>
<td>Location Services (LCS); Broadcast network assistance for E-OTD and GPS positioning methods</td>
</tr>
<tr>
<td>TS 04.71</td>
<td>Location Services (LCS); Mobile radio interface layer 3 specification</td>
</tr>
<tr>
<td>TS 08.31</td>
<td>Location Services LCS: Serving Mobile Location Centre - Serving Mobile Location Centre (SMLC - SMLC) interface; Stage 2</td>
</tr>
<tr>
<td>TS 08.71</td>
<td>Location Services (LCS); Base Station System Application Part LCS Extension (BSSAP-LE)</td>
</tr>
<tr>
<td>TS 09.31</td>
<td>Location Services (LCS); Location services management</td>
</tr>
<tr>
<td>TS 22.071</td>
<td>Location Services (LCS); Stage 1</td>
</tr>
<tr>
<td>TS 22.935</td>
<td>Feasibility study on Location Services (LCS) for Wireless Local Area Network (WLAN) interworking</td>
</tr>
<tr>
<td>TS 23.012</td>
<td>Location management procedures</td>
</tr>
<tr>
<td>TS 23.311</td>
<td>Gateway Location Register (GLR); Stage 2</td>
</tr>
<tr>
<td>TS 23.271</td>
<td>Location Services (LCS); Functional description; Stage 2</td>
</tr>
<tr>
<td>TS 23.635</td>
<td>Study into applicability of Galileo in Location Services (LCS)</td>
</tr>
<tr>
<td>TS 23.835</td>
<td>Enhanced support for user privacy in Location Services (LCS)</td>
</tr>
<tr>
<td>TS 24.030</td>
<td>Location Services (LCS); Supplementary service operations; Stage 3</td>
</tr>
<tr>
<td>TS 24.311</td>
<td>Requirements for support of Assisted Global Positioning System (A-GPS); Frequency Division Duplex (FDD)</td>
</tr>
<tr>
<td>TS 25.305</td>
<td>User Equipment (UE) positioning in Universal Terrestrial Radio Access Network (UTRAN); Stage 2</td>
</tr>
<tr>
<td>TS 25.453</td>
<td>UTRAN Iupc interface Positioning Calculation Application Part (PCAP) signalling</td>
</tr>
<tr>
<td>TS 25.657</td>
<td>UE positioning enhancements</td>
</tr>
<tr>
<td>TS 25.859</td>
<td>User Equipment (UE) positioning enhancements for 1.28 Mbps TDD</td>
</tr>
<tr>
<td>TS 29.199-9</td>
<td>Open Service Access (OSA); Parlay X Web Services; Part 9: Terminal location</td>
</tr>
<tr>
<td>TS 32.271</td>
<td>Telecommunication management; Charging management; Location Services (LCS) charging</td>
</tr>
<tr>
<td>TS 43.059</td>
<td>Functional stage 2 description of Location Services (LCS) in GERAN</td>
</tr>
<tr>
<td>TS 44.031</td>
<td>Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource</td>
</tr>
<tr>
<td>TS 44.035</td>
<td>Location Services (LCS); Broadcast network assistance for E-OTD and GPS positioning methods</td>
</tr>
<tr>
<td>TS 44.071</td>
<td>Location Services (LCS); Mobile radio interface layer 3 LCS specification</td>
</tr>
<tr>
<td>TS 48.031</td>
<td>Location Services LCS: Serving Mobile Location Centre - Serving Mobile Location Centre (SMLC - SMLC) interface; Stage 2</td>
</tr>
<tr>
<td>TS 49.031</td>
<td>Location Services (LCS); Base Station System Application Part LCS Extension (BSSAP-LE)</td>
</tr>
</tbody>
</table>

**Home Location Register (HLR)**

The HLR is the location register that administers all important permanent subscriber information. In addition, temporary subscriber information such as the currently serving VLR (see below) is stored. Serving as information desk for the user’s whereabouts, the HLR is the enabling entity to support roaming and macro-mobility.

Services as supported by HIS concentrate on micro-mobility for which the HLR has no direct relevance in the scope of this work.

**Visitor Location Register (VLR)**

The VLR is the location register for circuit switched services used for MSC controlled roaming of calls to or from mobile stations currently located in its area. Positioning is supported on location area basis comprising one or more cells. HIS services that sufficiently rely on rough position estimates only, comparable to granularities of Cell Id based localization (see Section 4.3.1), may be based on VLR information.
Granularity may be improved if the Location Service feature is supported. Storage of location data with timestamps further allows application of HIS filtering with respect to short-, mid- and long-term data (see Section 5.4.2.2.)

**Serving GPRS Support Node (SGSN)**
The location register function in the SGSN stores subscription information and location information for packet switched services. It represents the logical counterpart to MSC/VLR for circuit switched services. HIS related aspects apply likewise.

**Gateway GPRS Support Node (GGSN)**
The location register function in the GGSN stores subscription information and routing information needed to tunnel packets destined for a GPRS MS to the SGSN where the MS is registered. The GGSN thus holds responsible for roaming and macro-mobility with no further direct impact on HIS services.

**5.6.1.2 Location Services (LCS)**
The previously introduced registers provide location support in the sense that the residence of a terminal is roughly known. While granularities in the range of the location area are well suited to support paging, value added services being based on the context ‘location’ need further sophistication. For this, a new feature called *Location Services* (LCS) was introduced with Release 99 and enhanced by subsequent 3GPP releases.

Offering the ability to localize a terminal, LCS is used to provide services to the end-user for emergency services or for ‘internal clients’. The latter could be a UMTS network entity like an RNC that uses location information to direct the beam for space diversity. On the one hand side, the Hybrid Information System as integrated part of the network inherently applies LCS services when mapping link state information to positions. On the other hand, HIS data may be used to improve positioning, making it part of the LCS feature itself.
With the definition of LCS, new entities and interfaces have been specified and introduced. Altogether, they establish a logical node LCS architecture. Figure 5.6 depicts the corresponding LCS enhancements, comprising GMLC, SMLC and LMU as new LCS entities. Furthermore, additional functionality was added to existing entities such as BSC/SRNC and CBC in order to deal with LCS. The tasks of these new LCS entities along with their relationship to the Hybrid Information System will be explained in the following.

**Gateway Mobile Location Center (GMLC)**

GMLC is the logical entity to connect external LCS clients to the LCS architecture. It performs registration authorization and requests routing information from the HLR. External location requests are forwarded to the visited MSC, from which returning location estimates are passed back to the external LCS client. Unless HIS related databases are not implemented in external entities, there is no direct relation between HIS functionality and the GMLC.
Base Station Controller/Serving Radio Network Controller (BSC/SRNC)
The BSC for GERAN and SRNC for UTRAN receive authenticated location requests from the CN.

- In UTRAN, the SRNC coordinates incoming positioning requests. It takes into account their priorities and selects the appropriate positioning method to fulfill the requested accuracy. It interfaces, when necessary, with the CRNC that mainly manages resources allocated to UE positioning operations and requests UE Positioning related measurements from its associated Node Bs and LMUs.
- In GERAN, the BSC passes the location request to the SMLC.

From a HIS perspective, functions being concerning with short-term data handling are involved.

Serving Mobile Location Center (SMLC)
The SMLC function can be part of the RNC or be a SAS (Stand-Alone SMLC) for UTRAN. For GERAN, the SMLC function can be part of the BSC or be in a separate SMLC server.

- In UTRAN, the SMLC function provides assistance data to the RNC and acts as a location calculation server if the location estimates are not to be calculated in the RNC.
- In GERAN, the SMLC function coordinates the positioning request, schedules resources required to perform positioning of a mobile, and calculates the final location estimate and accuracy. The SMLC may control a number of LMUs.

HIS related tasks comprise the calculation of terminal positions and provisioning of location specific assistance data.

Location Measurement Unit (LMU)
The LMU entity that is placed at a fixed position is needed for reference measurements of radio signals. HIS needs to interact with the position signal measurement function of the LMU.

Cell Broadcast Center (CBC)
In GERAN, the SMLC function may interface a CBC in order to broadcast assistance data using existing cell broadcast capabilities. Applicability in UTRAN is for further study within 3GPP.
HIS may incorporate broadcast services to announce its disposition. In addition, location based addressing schemes such as geo-multicast could be supported by HIS-CBC interworking. The LCS service is provided by interaction of dedicated functional entities, which are grouped and sub-grouped as

- The *LCS Client* functional group
  - Location Client Functions
    - External Location Client Function (*LCF*)  
      \[\text{relevant for HIS}\]
    - Internal Location Client Function (*U-LCF*)  
      \[\text{relevant for HIS}\]

- The *LCS Server* functional group
  - Client Handling Component
    - Location Client Control Function (*LCCF*)
    - Location Client Authorization Function (*LCAF*)
    - Location Client Coordinate Transformation Function (*LCCTF*)  
      \[\text{relevant for HIS}\]
    - Location Client Zone Transformation Function (*LCZTF*)  
      \[\text{relevant for HIS}\]
  - System Handling Component
    - Location System Control Function (*LSCF*)
    - Location System Billing Function (*LSBF*)
    - Location System Operations Function (*LSOF*)  
      \[\text{relevant for HIS}\]
    - Location System Broadcast Function (*LSBcF*)
  - Subscriber Handling Component
    - Location Subscriber Authorization Function (*LSAF*)
    - Location Subscriber Privacy Function (*LSPF*)
  - Positioning Component
    - Positioning Radio Coordination/Control Function (*PRCF*)
    - Positioning Radio Assistance Function (*PRAF*, GSM only)
    - Positioning Calculation Function (*PCF*)  
      \[\text{relevant for HIS}\]
    - Positioning Signal Measurement Function (*PSMF*)  
      \[\text{relevant for HIS}\]
- Positioning Radio Resource Management (PRRM, UMTS only) \(\rightarrow\) relevant for HIS

The above given listing of location functions points up that not all functions are needed for the realization of the Hybrid Information System. Hence, the following description restricts to HIS relevant functions only. An exhaustive description on location services, entities and interfaces is provided in [175] for UTRAN and [176] for GERAN, respectively.

Table 5.3 provides a description of selected LCS functions and indicates the context in which their application is relevant for the Hybrid Information System.

**Table 5.3: Selected LCS functions and relation to HIS**

<table>
<thead>
<tr>
<th>3GPP LCS Function</th>
<th>Task</th>
<th>Relevance for HIS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location Client Functions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCF</td>
<td>Logical interface between external LCS client and internal LCS server Requesting ME/UE specific location information</td>
<td>Only needed, if HIS shall be realized as external entity</td>
</tr>
<tr>
<td>U-LCF</td>
<td>Logical LCS interface (internal) Use of location information for internal operations, e.g., location assisted handover</td>
<td>Feeding of HIS depends on U-LCF function</td>
</tr>
<tr>
<td><strong>Client Handling component</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCCTF</td>
<td>Conversion of location estimate from universal latitude/longitude system to local geographic system</td>
<td>Enables HIS to process arbitrary location information</td>
</tr>
<tr>
<td>LCZTF</td>
<td>Transformation of location into US zone identity (emergency service)</td>
<td>Only needed for integrated HIS-E911 deployment</td>
</tr>
<tr>
<td><strong>System Handling component</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LSOF</td>
<td>Provisioning of data, positioning capabilities Client data, subscription data Validation, fault management Performance management</td>
<td>HIS support for improved positioning (accuracy &amp; precision) Location-based handover support</td>
</tr>
<tr>
<td><strong>Subscriber Handling component</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Positioning Component</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Table:** Realization Aspects: Mapping to 3/4G Architectures

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCF</td>
<td>Calculation of mobile position through Algorithmic computation on collected measurements → accuracy. Conversion of location between different geodetic systems. Position tracking and prediction. Joint evaluation from different location measurement sources to improve accuracy &amp; precision. Smoothing of inherent positioning errors.</td>
</tr>
<tr>
<td>PSMF</td>
<td>Performing and gathering of radio signal measurements. Gathering of combined location data and measurement.</td>
</tr>
<tr>
<td>PRRM</td>
<td>Managing the effect of LCS operations on the overall performance of the system. Control variation of signal power level due to LCS application; calculate interference due to positioning operations; co-operate with CAC/RRM control timing aspects. Co-ordination among RNCs. Trigger generation for (V)HO needs to consider overall framework.</td>
</tr>
</tbody>
</table>

**Figure 5.7: Location Service functions and relation to HIS**

In order to be able to classify which LCS function is assigned to which network element, a respective mapping was compiled in Figure 5.7. However, the presented mapping of HIS functionality onto specific entities has a suggestive character only. Implementations may be different: Some particular functions may be
gathered in the same equipment for which related interfaces may become internal.

One can see that HIS related functions essentially are split between core network and access network. Related functions in the terminal are implemented within a logical peer entity but are not part of the actual Hybrid Information System. Due to Table 5.3 and Figure 5.7, HIS is not involved in any subscriber handling process. Classical tasks here comprise authorization and privacy handling being out of focus of the Hybrid Information System. For some general remarks with respect to location and privacy, please see Section 4.1.2.3.

Similarly, system handling is also not in HIS either. Specific functions here comprise system control and billing. Since the Hybrid Information System is supposed to be deployed on top of existing infrastructures, it is assumed that all relevant system handling functions are present anyway, hence being non-dependent on any HIS interaction.

Client handling support is restricted mainly to internal use. HIS is conceived to complement and improve LCS services. From a network internal point of view, this results in support of e.g., handover by means of triggering. External clients however, e.g., context aware applications being dependent on improved location accuracy due to HIS, are served by the GMLC via the Le interface.

Most interaction between HIS and 3GPP LCS functional entities is given for positioning support. Implementation of the Position Calculation Function (PCF) within HIS, for example, allows for self-contained calculation of the terminal position. However, even if an initial calculation was carried out by a PCF being resided e.g., in the SMLC, HIS would be able to improve accuracy by joint evaluation from different location measurement sources. Another means to improve LCS based positioning is to apply HIS based position tracking and prediction. Monitoring a terminal’s movement allows for derivation of a priori knowledge in terms of possible future whereabouts. This information in turn may be used for smoothing of inherent measurement positioning errors.

A comprehensive overview of the 3G network architecture with all related LCS entities and functions was compiled in Figure 5.6. Black boxes depict standard 3GPP interfaces/reference points. Red (dashed) boxes stand for entities and interfaces being introduced by 3GPP to realize the LCS feature, whereby the figure includes only relevant functions as described in Table 5.3.
The Hybrid Information System logically is arranged at the \( Iu \) interface of radio access network and core network, which is inline with the presentation in Figure 5.7. Respective interfaces for e.g., triggering and data exchange are included in Figure 5.6 as blue (dashed-dotted) connections. HIS entails all logical LCS functions, whereas their counterparts have been associated to their corresponding entities. Depending on the chosen HIS realization approach, centralized or distributed, HIS interacts and controls, respectively mirrors specific entities. It is to note that Figure 5.6 depicts one single HIS instance only. Since handover is a local decision aspect, it is recommended to scale a possible deployment in a similar manner as cell management is done. For example, one HIS instance should be restricted to manage a few BSCs/SRNCs only. The arising benefit is threefold: First, databases as administered by HIS are kept accurately small; second, signaling traffic and data exchange is minimized and third, time critical decision-taking actions are accelerated. The general doctrine is to place functions and related entities the ‘closer’ to the air interface the more time critical they are. This is also indicated in Figure 5.6: While short-term databases need to be present as part of the radio access network, long-term databases may be sourced out to any associated system to be accessed via backbone connections.

5.6.2 WLAN/3GPP Interworking Architecture

Starting with Release 6, 3GPP is on the way to standardize WLAN/3GPP interworking that allows terminals to access 3GPP services via WLAN (TR 23.234, 3GPP system to WLAN interworking) [24]. However, the scope of this specification does not target on optimal network selection with respect to ‘always best connected’ automation. The main reason for WLAN integration within the 3GPP efforts is to integrate WLAN as a complementary radio access in order to provide enhanced 3GPP (core network) services, exemplary done in [177] presenting a proposal for the tight coupling integration of WLAN-based Media Points and 3GPP/UMTS systems. Hence, the approach followed is an operator centric one. Obviously, one of the main concerns of WLAN/3GPP interworking addresses AAA aspects, since access via WLAN shall not circumvent 3GPP based radio access.

Figure 5.8 depicts the corresponding reference model for WLAN access to 3GPP services as specified in [24]. The user centric approach followed by HIS including VHO to possibly competing operators results in fewer realization aspects for HIS in this RM compared to the 3GPP LCS architecture presented in Section
5.6.1. Nonetheless, due to position tracking and prediction, HIS may support and speed up the authentication process controlled by the 3GPP AAA Server. The necessity for latency minimization requires anticipation, e.g., by means of pre-warming zones, see Section 3.3.2.6, a service possibly provided by HIS. Position tracking further allows for new charging models based on the location, cp. Annex A.5. Accordingly, HIS offers support for Online/Offline Charging Systems, too.

The interworking architecture of 3GPP further addresses the problem of initial network selection. For this, the Universal Integrated Circuit Card (UICC)\textsuperscript{26} in the terminal administers preference lists of PLMN and WLAN operators. There are two types of lists: User controlled and operator controlled ones. Since it is possible to update those lists via the air-interface, HIS can support and speed up the network selection procedure by providing up-to-date entries, whenever \textit{any} network connection (WLAN or 3GPP) is active. In addition to information on sole existence of serving networks, additional value-adding information can be provided, e.g., applied scrambling code in a particular UMTS cell, refer to Section 5.5 for further examples of HIS support applications.

Finally, personalized network access is an interesting service to be supported. Due to HIS’ data exchange with HSS/HLR, it is possible to consider user preferences when updating PLMN/WLAN network access lists.

\textsuperscript{26} The UICC chip card is an essential component for UMTS, just as the SIM is for GSM. Besides containing the USIM application, it provides a platform for other IC Card applications with secure support for all kinds of multi-application schemes.
5.6.3 WINNER Logical Node Architecture

Ongoing research within integrated projects of the 6th European Framework Programme yields on defining B3G overall system concepts. One of those integrated projects is WINNER that was introduced in Section 3.2.2.12. Since substantial parts of this thesis have been incorporated into WINNER, the following section addresses realization aspects of the Hybrid Information System as part of the WINNER system architecture.

The WINNER Logical Node Architecture Model [111] is shown in Figure 5.9. The aim is to design a platform for realizing the vision of ubiquitous system concept providing access with one single system. The number of logical nodes and interfaces thereby shall be kept sufficiently small. In general, WINNER defines a logical node as an entity in the (radio access) network that terminates a certain set of protocols [111]. Contrary to this, a physical node denotes a physically existing device in the network that incorporates certain functionality, thereby representing one or possibly more logical nodes. From the WINNER perspective, the Hybrid Information System as proposed within this work hence can be interpreted as interaction of physical entities, each being responsible for support of a specific service or function. This definition does not prescribe whether HIS needs to be implemented in a centralized or distributed way, cp. Section 5.6, since despite of defining protocol termination points, the WINNER
logical node architecture model does not suggest a certain physical placement of functional entities.

So far$^{27}$, the WINNER architecture defines six logical nodes: UT, RN, AP, RANG, ACS and AR [111].

**User Terminal Logical Node** ($\text{UT}_{\text{LN}}$) is a logical node comprising all functionality necessary for it to communicate directly with another UT or the radio access network.

**Relay Node Logical Node** ($\text{RN}_{\text{LN}}$) is a logical network node with relaying capabilities that is wirelessly connected to an $\text{AP}_{\text{LN}}$, $\text{UT}_{\text{LN}}$ or another $\text{RN}_{\text{LN}}$. Hence, one major difference to an $\text{AP}_{\text{LN}}$ is that it does not terminate any transport layer protocols.

**Access Point Logical Node** ($\text{AP}_{\text{LN}}$) is a logical node terminating the transport layer protocols on the network side as well as mode specific radio protocols on the UT side.

**Radio Access Network Gateway Logical Node** ($\text{RANG}_{\text{LN}}$) is a logical network node that terminates L2 protocols. More specifically, it terminates generic data link layer protocols of the *user plane*.

**Access Control Server Logical Node** ($\text{ACS}_{\text{LN}}$) is a logical network node that controls the access to the radio interface resources. It terminates generic *control plane* protocols.

**Access Router Logical Node** ($\text{AR}_{\text{LN}}$) is a logical IP layer node that performs the tasks attributed to an access router as defined in relevant IETF specifications.

$^{27}$ Due to ongoing definition of the WINNER system and related protocols, further refinement of the given logical nodes is possible.
Figure 5.9: WINNER Logical Node Architecture and relation to HIS

Depending on the deployment scenario to be covered, WINNER specifies several distinct modes on a common basis. Each mode thereby is tailored to the needs of different radio environments. Key aspects being common to all modes are concentrated within generic functions while specific functions are tailored to dedicated scenarios. In general, the WINNER logical nodes 'close' to the air interface such as AP/BS control specific functions, while generic functions are handled by RANG and ACS logical nodes in the core network. The latter two entities further distinguish in their responsibilities in the way that RANG terminates user plane protocols while ACS terminates control plane protocols, see Table 5.4.

Table 5.4: HIS related to WINNER Logical Node Architecture

<table>
<thead>
<tr>
<th>Mode Control</th>
<th>User Plane</th>
<th>Control Plane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic</td>
<td>RANG</td>
<td>ACS</td>
</tr>
<tr>
<td>Specific</td>
<td>AP</td>
<td>HIS</td>
</tr>
</tbody>
</table>

Being designed to provide support for system control, the Hybrid Information Systems is settled in the control plane. Due to short term information provisioning as indicated in Figure 5.9, HIS may be involved in e.g., link adaptation procedures, for which parts of the HIS functionality in Table 5.4 have been assigned
to specific mode support. However, most of the generic functions indicated in the top right box of Figure 5.9 belong to the generic functions of the control plane. Accordingly, HIS is likely to implement physical entities belonging to the ACS logical node.

The WINNER ubiquitous radio system is envisioned to adapt to different deployment scenarios and radio environments by using intelligent mode selection and switching between modes [112]. From a certain point of view, this task is similar to vertical handover triggering with a very tight coupling of involved systems. Within WINNER, a handover decision entity and a trigger entity have been defined, see Figure 5.9. Mapping the WINNER architecture to HIS functionality, this is exactly what is performed within the HIS Service Control Unit block, see Figure 5.9. Further mappings apply for the HIS Data Administration block with the ACS’ measurements entity and RATs monitoring & filtering entity.

5.6.4 Summary

Within this Section, HIS functionality was mapped to concrete systems designs giving a more complete picture of realization aspects with respect to HIS. Each architecture inherently addresses a specific topic: The 3GPP Location Architecture puts the focus on support of Location Services (LCS), the 3GPP/WLAN Interworking Architecture addresses mainly AAA aspects and the WINNER Logical Node Architecture deals with intra-system/inter-mode and inter-system/VHO management.

For all the three discussed system architectures, intersections with HIS properties have been worked out and presented. Figure 5.10 summarizes properties as described for the three different architectures and illustrates their corresponding affiliation from the HIS perspective. Support of different location features (PSMF, LCF, PCF, LCCTF...) as described for the 3GPP Location Architecture in Section 5.6.1, PLMN/WLAN list administration and location based AAA support as described for the 3GPP/WLAN Interworking Architecture in Section 5.6.2, as well as ACS relations of the WINNER Logical Node Architecture as derived in Section 5.6.3, can be recognized.

Two HIS Service Access Points (SAP) being connected to the Data Administration Unit and the Service Control Unit allow for requesting services from or by
HIS. Further interaction with other entities such as HSS, RNC or others is indicated by dashed line interconnections to respective entities outside the actual HIS block.

Figure 5.10: Mapping of different system architecture aspects to HIS

The implementation of HIS related functions may be performed in a centralized or distributed manner. For the centralized approach, HIS functionality is likely to
be implemented in a single physical unit. Respective entities are HIS internal, allowing for enclosed system control but obviously at the cost of increased complexity, more core network traffic and less scalability. The distributed approach restricts to a logical HIS node including some physical HIS management entities only. Actual data administration stays with network entities that maintain respective registers anyway. Evaluation of the two implementation forms is scenario dependent and out of scope of this thesis.
CHAPTER 6

Performance Analysis

Content

6.1 Localization Aspects ................................................................................................. 172
6.2 Correlation Analysis ................................................................................................. 176
6.3 Virtual Coverage ....................................................................................................... 182
6.4 Beacon Protection ..................................................................................................... 185

Keywords: Location Error, Modeling, Correlation, Cut-off criterion, Virtual Coverage, Proxy Buffering

The following chapter addresses aspects of imprecise positioning, service continuation in case of non area-wide Hot Spot coverage and harmful impacts of beacon broadcasts.

If measurements shall be concatenated with position information deriving from non-perfect localization, emerging errors need to be modeled. Assuming a large number of input data, it is straightforward to apply stochastic error distributions. Subsequent correlation analysis of erroneous and actual position data helps estimating reliability of location data based decision making.

Besides location aspects, service continuation is another topic. It is investigated, in how far proxy buffering in combination with UMTS is applicable to support specific high bit rate services for scenarios with only partial WLAN coverage. Related results may serve as basis for future WLAN deployment on the one hand, or worthwhile VHO triggering for existing deployments on the other hand.

The last topic to be addressed considers beaconing in WLAN systems. It will be shown that beacon protection as defined by 802.11e results in wasted capacity. A heterogeneous system environment under control of HIS, however, is able to counterbalance this drawback.
6.1 Localization Aspects

Localization is an important aspect in the scope of this work. Depending on the applied positioning technique, location estimations result in more or less accurate and precise outcome (for more details on accuracy and precision see Section 4.5). Within upcoming investigations, imprecise positioning is assumed according to settings being derived in the following section.

6.1.1 Modeling of Localization Imprecision

While error-free localization supplies exact position data, e.g., Cartesian coordinates $x_0, y_0, z_0$, location imprecision results in fuzzy location data spanning a position space $x_0 + \Delta x, y_0 + \Delta y$ and $z_0 + \Delta z$. Statistical handling allows for definition of spatial probabilities to describe this position space. Assuming a sufficiently large number of probes, the position probability density function is derived characterizing the location error. This in turn means that if the error distribution is known, erroneous positions can be generated from the exact positions, to be used within simulation runs.

Figure 6.1 exemplarily depicts the generation of erroneous location data. A terminal’s actual position is referred to as position (A). Depending on the applied localization method, different accuracies and precisions may be realized. Accuracy is modeled by a circle with radius $R$ around position (A). Precision is reflected by the probability that the estimated position (B) lies within $R$. Summarizing this, position (A) represents the real terminal location, whereas position (B) represents the estimated position resulting from erroneous localization.
Figure 6.1: Modeling of location imprecision based on error distributions

An important aspect within this thesis is the concatenation of measurement reports with related position information for subsequent processing. Whenever terminals provide measurement reports, the real position (A) is determined and used as reference in the evaluation process. In addition, an estimated position (B) can be drawn whose location error follows a specific error distribution. In principle, the underlying distribution can be of arbitrary nature, e.g., Rayleigh, Gaussian, or Uniform as indicated in Figure 6.1. The impact of different distributions, e.g., with respect to the reliability of location based networking, has also been investigated and published by the author in [104][105] but is not further elaborated within this thesis. For all upcoming investigations, a two-dimensional Gaussian error distribution with non-correlated deviations in x- and y-direction will be applied.

Figure 6.2 and Figure 6.3 exemplarily depict simulated ‘measurements’ whose associated positions differ from the exact ones due to erroneous positioning. For each real position (A) in Figure 6.1, a number of n = 1000 (Figure 6.2 a) respectively n = 100 (Figure 6.3 a) erroneous positions (B) have been drawn. The standard deviation is \( \sigma_x = \sigma_y = 10 \text{ m} \) and the chosen mean positioning error is \( \mu_x = \mu_y = 0 \text{ m} \). Moving away from the AP, new measurements are reported every
step size $s = 10 \text{ m}$, see Figure 6.2 b) and Figure 6.3 b). Figure 6.2 c) and Figure 6.3 c) depict the total error distribution of reported positions for the simulation run. The resulting distribution is a two-dimensional Gaussian.

![Figure 6.2: Measurements at real (A) and erroneous (B) position](n = 1000, no max error)

![Figure 6.3: Measurements at real (A) and erroneous (B) positions](n = 100, no max error)

### 6.1.2 Evaluation Criterion

For the evaluation of localization effects and to assess the similarity of radio conditions, say reception power $R_x$, at real (A) and estimated (B) location, an objective measure is needed. This can be provided by a cross correlation of respective measurement reports as taken at both positions, (A) and (B). Being based on statistical input parameters, the following evaluation is not restricted to one particular localization method but holds for any (combination of) position-
In probability theory and statistics, the covariance is a measure for the interrelation of two random variables X and Y. The covariance is positive if X and Y tend to result in a unitary linear interrelation. Negative values indicate antithetic properties and a value corresponding to zero means that no interrelation can be stated\(^\text{28}\). Since the covariance varies with the applied measurement unit, normalization is applied resulting in the definition of correlation. The statistical measure applied is the correlation coefficient \(\rho\). Perfect correlation is given for a value of +1 while perfect inverse correlation is indicated by a value of −1. Though different definitions of the correlation coefficient exist, the most widespread one is the Bravais-Pearson product-moment correlation coefficient, which is found by dividing the covariance of the two variables X and Y by the product of their standard deviations \(\sigma_X\) and \(\sigma_Y\). Accordingly, the correlation \(\rho_{XY}\) between two random variables \(X\) and \(Y\) with expected values \(\mu_X\) and \(\mu_Y\) and standard deviations \(\sigma_X\) and \(\sigma_Y\) is defined\(^\text{[103]}\) as:

\[
\rho_{X,Y} = \frac{\text{cov}(X, Y)}{\sqrt{\text{Var}(X)} \sqrt{\text{Var}(Y)}} = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y} \tag{6.1}
\]

Since \(\mu_X = E(X), \sigma_X^2 = E(X^2) - E^2(X)\) and \(\mu_Y = E(Y), \sigma_Y^2 = E(Y^2) - E^2(Y)\), equation (6.1) may be written as:

\[
\rho_{X,Y} = \frac{E(XY) - E(X)E(Y)}{\sqrt{E(X^2) - E^2(X)} \sqrt{E(Y^2) - E^2(Y)}} \tag{6.2}
\]

Equations (6.1) and (6.2) are based on knowledge of the entire subset of the random variates for which \(\rho_{XY}\) is referred to as the theoretical correlation coefficient. If the variables \(X, Y\) are based on a series of \(n\) measurements \(x_1, x_2, ..., x_n\) and \(y_1, y_2, ..., y_n\), correlation analysis is performed with the help of the so called empirical or sample correlation coefficient \(r_{X,Y}\)\(^\text{[103]}\) that calculates as

\(^{28}\)Covariance calculations resulting in zero do not exclude other interrelations between two probes ("null hypothesis"), e.g., Fibonacci values and their order feature by low covariance values though being deterministically determined.
6. Performance Analysis

\[ r_{X,Y} = \frac{\sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}} \]  \hspace{1cm} (6.3)

with the empirical expected values

\[ \bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \quad \text{and} \quad \bar{y} = \frac{1}{n} \sum_{i=1}^{n} y_i . \]  \hspace{1cm} (6.4)

Within signal theory [102], a slightly modified correlation coefficient \( c_{X,Y} \) is used. Zero-mean property is often required within signal analysis resulting in the definition (6.5):

\[ c_{X,Y} = \frac{\sum_{i=1}^{n} x_i y_i}{\sqrt{\sum_{i=1}^{n} x_i^2} \sqrt{\sum_{i=1}^{n} y_i^2}} \]  \hspace{1cm} (6.5)

Since the positioning error is assumed sufficiently small compared to the overall distance to the AP, \( R_{X,Y} \) probes taken at both positions (A) and (B) follow the correlation requirement for almost linear interdependency.

6.2 Correlation Analysis

The scenario in Figure 6.1 is now used to study the influence of the distance between AP and terminal on the correlation value. Initially placed close to a fixed AP, the terminal departs until coverage of the AP is exceeded. For the given scenario, an upper limit of \( D = 200 \) m adjusts, whereby a simple one slope path-loss model with an exponential attenuation factor of \( \gamma = 2.4 \) was applied (a more detailed description is provided in the simulation chapter 8.3.1.1). Further system related properties, especially the determination of measurement reports in terms of RPI levels (Received Power Indicator = quantized measure of received power) follow the recommendation of WLAN 802.11a, h [69][74]. Every 10 m the terminal has moved away from the AP, a series of \( n \) samples for the real po-
Correlation Analysis

The location error is assumed normally distributed with standard deviations of $\sigma_x = \sigma_y = 10$ m. Hereafter, the correlation coefficients $r_{X,Y}$ and $c_{X,Y}$ are calculated.

![Graphs showing distance related correlation](image)

**Figure 6.4: Distance related correlation $r_{X,Y}$ and $c_{X,Y}$ for $n$ samples per step**

Figure 6.4 shows the distance dependent correlation values $r_{X,Y}$ and $c_{X,Y}$ according to equations (6.3) and (6.5). Since the empirical correlation coefficient $r_{X,Y}$ considers variations of the mean value of the probe, the curve entails jerky leaps for a small number of $n = 10$ samples per step. With increasing number of samples, single outliers within the positioning process exert less influence on the correlation result. For $n = 100$ samples there is only one single gap for $r_{X,Y}$ at $D = 75$ m. For $n = 1000$, both curves are characterized by a monotonously increasing correlation while matching each other quite well.

Since long-term databases as administered by HIS dispose of a sufficiently large number of entries, the following correlation results are based solely on the correlation value $c_{X,Y}$ of equation (6.5).

In general, the correlation between measured $R_x$ values at real positions (A) and erroneous positions (B) increases with increasing distance to the transmitting station. This can be explained with the negative exponential attenuation characteristic. Close to the sender, localization imprecision has a higher impact on the measured $R_x$ level than far away. Thus, if the same reliability shall be given, localization in the centre of a cell needs to apply more sophisticated algorithms than at the cell border. On the other hand, if the same localization method is applied for nearby and for far-off terminals, location data based decision algorithms can rely better and better on respective data the more the terminal resides close to the cell edge. This is of particular interest for e.g., handover control that affects terminals, which are leaving the actual coverage area.
6.2.1 Normal Distribution with cut-off

Assuming location errors being normally distributed comprises probes with arbitrary distance to the actual position. Though the probability of extreme outliers is rather small, the mathematical model needs to be adjusted to reflect real radio conditions more precisely. Accordingly, the so-called cut-off distance $r_{cut}$ is defined that limits the maximum possible positioning error. Justification of $r_{cut}$ is given because unreasonably high positioning errors beyond $r_{cut}$ can be filtered out, e.g., by means of higher layer detection. This is realistic in the sense that measurement reports associated with a rather unlikely position being e.g., 1000 m away from the AP would be dropped as well. Comparison of the BSSID allows table driven derivation of the AP’s coordinates making it easy for higher layer algorithms to sort out misleading tuples of measurement and position. Depending on the applied positioning scheme, the cut-off value may scale down to some meters only.

The impact of restricting the maximum possible error is investigated in the following, see Figure 6.5. For better visualization, the one-dimensional case is shown, whereas respective considerations apply for the second dimension likewise.

![Figure 6.5: One dimensional Normal Distribution with cut-off](image-url)
In the example, localization error generation initially is based on a one-dimensional normal distribution with zero mean $\mu_{\text{orig}} = 0$ and standard deviation $\sigma_{\text{orig}}$. Due to the cut-off criterion, location errors for positions $| \pm x | > r_{\text{cut}}$ are discarded. Instead, new probes are generated until the cut-off condition is satisfied. Since generation of new probes applies the same parameters $\mu_{\text{orig}}$ and $\sigma_{\text{orig}}$, the resulting error-distribution remains zero-mean. However, it is shifted in $y$-direction and features a taller shape, see Figure 6.5. The cut-off areas $F_{\text{cut1}}$ and $F_{\text{cut2}}$ left and right from $x = \pm r_{\text{cut}}$ correspond to the areas $F_1$ and $F_2$ enclosed by the two graphs. Equation (6.6) shows the probability density function for the absolute value of the positioning error:

$$p(x) = \begin{cases} \frac{C}{\sqrt{2\pi}\sigma_{\text{orig}}} e^{-\frac{x^2}{2\sigma_{\text{orig}}}} & \text{for } -x_{\text{max}} \leq x \leq x_{\text{max}} \\ 0 & \text{otherwise} \end{cases} \quad (6.6)$$

In order to derive an estimation for the modified cut-off distribution represented by the new graph, the following approach was chosen: To obtain a valid probability density function it must be ensured that its integral equals one, see equation (6.7). $C$ is a term that needs to be introduced in order to compensate for the cut-off area and to obtain a valid PDF. It can be determined using:

$$\int_{-\infty}^{\infty} p(x)dx = 1 \quad (6.7)$$

By solving this equation, $C$ can be calculated according to (6.8),

$$C = \frac{2}{\text{erf} \left( \frac{-x_{\text{max}}}{\sqrt{2\sigma_{\text{orig}}}}, \frac{x_{\text{max}}}{\sqrt{2\sigma_{\text{orig}}}} \right)} \quad (6.8)$$

including the general error function $\text{erf}(a,b)$ whose definition is given by the integral

$$\text{erf}(a) = \frac{2}{\sqrt{\pi}} \int_{0}^{a} e^{-\tau^2} d\tau; \quad \text{erf}(b) = \frac{2}{\sqrt{\pi}} \int_{0}^{b} e^{-\tau^2} d\tau$$

$$\text{erf}(a,b) = \text{erf}(b) - \text{erf}(a) = \frac{2}{\sqrt{\pi}} \int_{a}^{b} e^{-\tau^2} d\tau \quad (6.9)$$

If the variance $\sigma_x^2$ shall be determined, it can be found by calculating:
\[ \sigma_x^2 = \int_{-\infty}^{\infty} p(x)x^2 \, dx \quad (6.10) \]

Thereby, \( \sigma_x^2 \) is the variance of the random variable with the probability density function as stated by (6.6). \( \sigma_{\text{orig}}^2 \) is the variance of the underlying zero-mean Gaussian distribution, which is cut-off at \( x_{\text{max}} \). Substituting \( p(x) \) with (6.6) gives:

\[ \sigma_x^2 = \int_{-x_{\text{max}}}^{x_{\text{max}}} \frac{C}{\sqrt{2\pi} \sigma_{\text{orig}}} \, e^{-\frac{x^2}{2\sigma_{\text{orig}}}} \, x^2 \, dx \quad (6.11) \]

Solving this and using (6.8) results to

\[ \sigma_x^2 = \frac{C}{\sqrt{2\pi}} \left( \sqrt{\frac{\pi}{2}} \sigma_{\text{orig}} \, \text{erf} \left( \frac{-x_{\text{max}}}{\sqrt{2} \sigma_{\text{orig}}} \right) \right) - 2e^{\frac{-x_{\text{max}}^2}{2\sigma_{\text{orig}}^2}} \sigma_{\text{orig}} x_{\text{max}} \quad (6.12) \]

with \( C \) as calculated in (6.8). Derivation of \( \sigma_x^2 \) is important for additional calculations based on a current set of erroneous position data. For instance, the introduction of position prediction by the Hybrid Information System using a Kalman Filter requires detailed knowledge of the measurement error’s covariance matrix. A detailed description of this topic has been published as related work in [76].

Figure 6.6 illustrates application of the cut-off criterion to the scenario given by Figure 6.1 and Figure 6.2. The introduction of the cut-off criterion limits the maximum possible location error. Due to rejection of statistical outliers, the resulting 2-D distribution appears more complex, i.e., its measurement density within the cut-off limits is increased.
6.2. Correlation Analysis

This effect is shown by Figure 6.7 that illustrates the 3D equivalent of Figure 6.2c) and Figure 6.5. Elimination of outliers leads to database entries that feature by different statistical properties compared to non-filtered input data. Applying the cut-off constraint to the scenario in Figure 6.1 with subsequent correlation evaluation results in increased interrelation the more stringent, i.e., smaller maximum position errors, the cut-off border is defined, see Figure 6.8.

Figure 6.7: Total error distribution without cut-off and cut-off at 20 m

Figure 6.8: Distance dependent correlation $c_{x,y}$ with cut-off thresholds

The definition of realistic cut-off borders is one out of many parameters to be chosen in simulations as presented in Section 8. It was stated in Section 4.5 that
accuracy and precision are two important parameters that reflect capabilities of localization methods. The introduction of the cut-off limit directly affects these values in the sense that accuracy is adjusted to the maximum possible error while at the same time precision rises to 100%. Unless stated otherwise, a default value of \( r_{\text{cut}} = 20 \) m was chosen as cut-off limit for upcoming simulations.

Another topic to be investigated in the next section concerns service continuity and proxy buffering. In spite of non area-wide Hot Spot coverage, it is possible to maintain specific high bit rate services that could not be supported by sole UMTS installations.

### 6.3 Virtual Coverage

Audio and video streaming services commonly require higher bandwidths than speech services. Since UMTS is not suited to carry many high bit-rate streaming services [125] (especially at the cell edge), wireless local area networks like 802.11 are candidate systems for complementing UMTS in Hot Spot areas. However, due to WLAN inherent low coverage, solutions for end-to-end service continuity using a combination of UMTS and WLAN need to be found.

Using buffering techniques, streaming services can be supported for certain amounts of time with reduced bandwidth available. Interesting caching strategies comprise the Media Point service concept as described in [126].

Patchy 802.11 coverage areas may be bridged by using UMTS to support services with reduced bandwidth. Figure 6.9 shows a Manhattan scenario with two access points placed at road crossings. The corresponding Hot Spots do not overlap, thus, MTs moving along the street will face an interruption of WLAN connectivity, and continuous transmission is only possible through the overlaid UMTS network. It is assumed that mobile users leaving AP1 coverage were able to fill completely their reception buffer. For initial investigations, the buffer size was chosen to cache 2000 packets carrying 160 Bytes each. When moving towards AP2, the service may be carried on simply by consuming buffered packets. Though UMTS supports only reduced data-rates, i.e., less than the actual service requires, the deceleration of buffer clearance due to interim UMTS connectivity allows for ongoing service provisioning.

From the applications point of view, no coverage termination is realized as long as there are still packets in the buffer to be consumed. The interpreted AP cell
size thus appears larger than it actually is, for which the notation virtual cell size or virtual coverage area is introduced. These results are compliant with ‘smart caching’ approaches as proposed in [127]. It is shown, that for non-real-time services a virtually continuous broadband connection is provided even in case of fragmentary network coverage.

It should be noted that the concept of virtuality cannot be applied to all services, but is restricted to streaming services and background traffic. The theoretical, ‘virtual’ coverage gain due to buffering is indicated in Figure 6.9 by \( d_{\text{Buffer}} \).

\[ \text{Figure 6.9: Virtually increased Cell Size using Buffering} \]

Thus, \( d_{\text{Buffer}} \) is the distance a certain service could further be maintained without switching to UMTS right after leaving the WLAN coverage. However, by performing vertical handover to the UMTS network, the service may be supported even longer, although UMTS itself is not able to carry the entire offered load required for that service. The additionally gained distance is indicated by \( d_{\text{UMTS}} \), see Figure 6.9. The related simulation chain together with the different buffers in use are depicted in Figure 6.10.

\[ \text{Figure 6.10: Transmission and Reception Buffers for virtual coverage} \]
The distance the terminal may move without the service breaking down is calculated by:

\[ d_{\text{max}} = d_{\text{Buffer}} + d_{\text{UMTS}} = \frac{L_Q}{\lambda_{\text{Service}} - \mu_{\text{UMTS}}} |v| \]  

Equation (6.13)

Table 6.1 shows exemplary distances for selected services. The data rate that is used within UMTS is assumed to \( \mu_{\text{UMTS}} = 64 \text{ kbit/s} \). The mobile terminal's velocity was set to 30 km/h. It can be seen that mobile users maintain audio stream services for a significant distance after leaving the WLAN Hot Spot. Video streams cannot be supported for long at that velocity.

**Table 6.1: Distance \( d_{\text{max}} \) to be bridged by buffering & VHO to UMTS**

<table>
<thead>
<tr>
<th>Service</th>
<th>Bit rate ( \lambda_{\text{Service}} )</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP3 Stream (avg.)</td>
<td>128 kbit/s</td>
<td>333 m</td>
</tr>
<tr>
<td>MP3 Stream (good)</td>
<td>256 kbit/s</td>
<td>111 m</td>
</tr>
<tr>
<td>Video Stream</td>
<td>2 Mbit/s</td>
<td>11 m</td>
</tr>
</tbody>
</table>

The previous investigation helps in deriving deployment rules for installation of WLAN technology. Assuming an overlay UMTS network, it is now possible to derive upper distance limits between adjacent APs, superseding the necessity for full coverage. On the other hand, if the distance of two already existing neighboring APs is known, one can estimate the best possible service (in terms of throughput) that still can be supported.

Finally, another advantage is given that has not been stated so far: It was shown that VHO to the UMTS overlay network makes sense, though UMTS only supports a fractional part of the bandwidth required by the service. By bridging the connectivity gap that buffering techniques cannot fill, non-interruptive service continuity is achieved. An important keyword here was *virtual* coverage. However, it is to point out that VHO to UMTS straight after leaving AP1’s coverage area means *real* coverage (better: connectivity), though at reduced bandwidth. Nonetheless, the effective radio connection may be used to convey not only user data but also control data. This enables session continuity making time consuming session re-establishment negotiations obsolete when entering AP2 coverage.
Related research has shown that elastic-buffering mechanisms in terrestrial networks bring significant advantages in terms of network effectiveness [77]. The results of this work may serve as basis for further investigations with respect to derivation of dimensioning rules for intermediate buffering. Since increased buffer sizes result in increased delay performance, proxy buffering is likely to focus on non real-time streaming services. Sophisticated handover schemes could incorporate buffer capacity and user velocity to decide whether VHO in partly covered areas due to Figure 6.9 allows for seamless service continuity or not.

The last topic to be addressed is about broadcast of system information. Specific mechanisms result in wasted capacity. Concepts presented in this work counterbalance this drawback by means of adaptive beaconing.

### 6.4 Beacon Protection

Every radio system comprises specific information channels used to provide associated terminals or terminals that are just about to associate with basic system information. While the realization of such information channels may differ, one common characteristic is their ongoing repetition on a periodical basis. Within WLAN 802.11, so-called Beacons are broadcasted to supply terminals with necessary system information. With the introduction of beacon protection in 802.11e, it is ensured that deterministic beacon broadcasting takes place. A detailed description of beacon based synchronization and cell search has been given in Section 2.2.2. While the beacon is of fundamental necessity for newly to associate terminals, its presence is not that important for already active terminals and may even be harmful in terms of wasted capacity. Stations with a valid TXOP that are not able to terminate an envisioned frame exchange prior to the next TBTT need to defer and generate non-used idle gaps\(^29\) of length \(T_{\text{offset}}\), see Figure 6.11.

---

\(^{29}\) Due to timing constraints, it is not possible to perform fragmentation (in order to avoid the idle-gap by sending only a fraction of the initially scheduled packet) once TXOP was granted. However, even if it was possible, other drawbacks arise resulting in inefficient protocol performance because of small packet fragments.
Figure 6.11: Idle gaps due to beacon protection

The resulting maximum overall throughput between two subsequent beacon transmissions ($\Delta$TBTT) depends on the duration for beacon transmission $T_{\text{beacon}}$ and the duration of the frame exchange sequence $T_{\text{transmission}}$. The latter comprises mean durations for channel access and guard times ($T_{\text{AIFS}}$, $T_{\text{backoff}}$, $T_{\text{SIFS}}$, $T_{\text{ACK}}$), and the actual frame duration $T_{\text{frame}}$, see inequation (6.14). Optionally, additional time $T_{\text{optional}}$ is needed if the RTS/CTS mechanism is applied.

$$T_{\text{beacon}} + N \left( T_{\text{AIFS}} + T_{\text{backoff}} + T_{\text{optional}} + T_{\text{frame}} + T_{\text{SIFS}} + T_{\text{ACK}} \right) < \Delta$TBTT$$

(6.14)

While $T_{\text{beacon}}$ needs to be considered only once at the beginning of each beacon interval, $T_{\text{transmission}}$ can take place $N$ times.

Actual user data is exclusively conveyed during $T_{\text{frame}}$ that can be further separated into a constant term $T_{\text{control}}$ and a variable term $T_{\text{data}}$. The applied transmission scheme for $T_{\text{data}}$ is not fix and may vary according to applied link adaptation schemes.
6.4. Beacon Protection

\[
T_{\text{frame}} = T_{\text{control}} + T_{\text{data}} = \frac{T_{\text{frame}}}{16 \mu s} + \frac{T_{\text{signal}}}{4 \mu s, BPSK1/2} + \frac{T_{\text{data}}}{BPSK1/2, BPSK3/4, \ldots} \quad (6.15)
\]

The duration of \( T_{\text{data}} \) depends on the number of required OFDM symbols \( \Sigma N_{\text{OFDM}} \) because the symbol duration \( T_{\text{symbol}} \) has a fixed length of 4 \( \mu s \).

\[
T_{\text{Data}} = \sum_{\text{Symbol}} N_{\text{OFDM}} \cdot T_{\text{Symbol}} \quad (6.16)
\]

The number of required OFDM symbols however, depends on the packet size \( N_{\text{PSDU}} \) (whose framebody entails the actual user data of lengths \( L_{\text{packet}} \)) and the applied PHY-Mode. \( N_{\text{DBPS}} \) is the PHY-Mode specific property that describes the coded bits per OFDM symbol. Hence, \( \Sigma N_{\text{OFDM}} \) is calculated by equation (6.17)

\[
\sum_{\text{Symbol}} N_{\text{OFDM}} = \frac{16\text{ bit}}{N_{\text{service}}} + \frac{MAC-\text{PDU}(s)}{Management, Control, Data} + \frac{6\text{ bit}}{N_{\text{PSDU}}} + N_{\text{tail}} + N_{\text{pad}} \quad (6.17)
\]

with \( N_{\text{DBPS}} \in \{24, 36, 48, 72, 96, 144, 192, 216\} \) and padding bits \( N_{\text{pad}} \) according to

\[
N_{\text{pad}} = N_{\text{DBPS}} - \left( \left( N_{\text{service}} + N_{\text{PSDU}} + N_{\text{tail}} \right) \mod N_{\text{DBPS}} \right). \quad (6.18)
\]

Neglecting constant terms and the variable but small amount of padding bits, the following relation applies based on (6.14) - (6.18):

\[
\frac{T_{\text{max}}(\Delta \text{TBTT})}{N(\Delta \text{TBTT})} > T_{\text{frame}} \sim T_{\text{data}} \sim \sum_{\text{Symbol}} N_{\text{OFDM}} \sim \frac{N_{\text{PSDU}}}{N_{\text{DBPS}}(\text{PHYMode})}. \quad (6.19)
\]

\( T_{\text{max}} \) within (6.19) indicates that there is an upper time limit, within which transmissions need to take place. \( N \) denotes the number of consecutive frame exchanges between two beacon transmissions. Both numbers depend on the given beacon interval \( \Delta \text{TBTT} \). Being a natural number (positive integer, i.e., \( N \))
\( \in \{1, 2, 3...\} \) and satisfying inequations (6.14) and (6.19), \( N \) can be calculated according to

\[
N = \text{floor} \left[ \frac{\Delta TBTT - T_{\text{beacon}}}{T_{\text{transmission}}} \right] \tag{6.20}
\]

The resulting user data throughput can be derived according to equation (6.21):

\[
TP_{\text{user}} = N \times \frac{L_{\text{packet}}}{\Delta TBTT} . \tag{6.21}
\]

Knowing the maximum number \( N \) of consecutive transmissions between two beacon broadcasts allows transferring inequation (6.14) into equation (6.22) by introducing \( T_{\text{offset}} \),

\[
T_{\text{beacon}} + N \times T_{\text{transmission}} + T_{\text{offset}} = \Delta TBTT , \tag{6.22}
\]

with \( 0 \leq T_{\text{offset}} < T_{\text{transmission}} \).

Substituting \( \Delta TBTT \) in equation (6.21) by equation (6.22) with subsequent re-arrangement of \( N \) results in equation (6.23).

\[
TP_{\text{user}} = \frac{L_{\text{packet}}}{\frac{T_{\text{beacon}}}{N} + \frac{T_{\text{transmission}}}{N} + \frac{T_{\text{offset}}}{N}} \tag{6.23}
\]

Based on equation (6.23), the following statements are derived:

1. The resulting user throughput \( TP_{\text{user}} \) increases with increasing packet sizes \( L_{\text{packet}} \);
2. The influence of the duration of the beacon transmission \( TP_{\text{beacon}} \) on the user throughput \( TP_{\text{user}} \) decreases with increasing beacon interval \( \Delta TBTT \) and hence increasing \( N \);
3. The influence of the idle-gaps \( T_{\text{offset}} \) on the user throughput \( TP_{\text{user}} \) decreases with increasing beacon interval \( \Delta TBTT \) and hence increasing \( N \).
The previous considerations show that beacon protection may harmfully affect user throughput due to resulting idle-gaps not being used for transmissions. Simulation results with respect to this topic will be presented in Section 8.5.1. It will be shown that simulation and analysis match quite well.

Once being aware of the negative influence of beacon protection on the user throughput, beacon adaptation strategies will be investigated. The proposed method is to apply the Hybrid Information System in order to perform *adaptive beaconing.*
CHAPTER 7

Integrated Simulation Environment

Content

7.1 Overview ................................................................. 191
7.2 S-WARP ................................................................. 193
7.3 URIS ................................................................. 196
7.4 S-GOOSE/RISE .................................................... 199
7.5 Extended HIS ...................................................... 200
7.6 Simulator Integration & Modeling ...................... 207
7.7 Simulator Validation ............................................ 209

Keywords: Protocol Simulator, Coupling, Modular Concept, Validation

The underlying concept of the Hybrid Information System (HIS) has been presented in Chapter 5. Key idea of HIS is to support interworking between heterogeneous networks by providing location related cross-system information. Within this work, the related concept has been developed from an initial idea to a concrete cooperation scheme. Realization aspects for applied system interworking and its implementation are the focus of the upcoming chapter. All performance evaluations and simulations as presented in Chapter 8 are based on the following simulator implementations and couplings.

7.1 Overview

To investigate the benefits of heterogeneous system interworking including the potentials introduced by vertical handover, different system models need to be combined.
Based on long-term experiences gained in various diploma/PhD theses and associated research, the Chair of Communication Networks (ComNets) has developed highly sophisticated simulation environments. Existing implementations
comprise specifications according to UMTS, GSM (GPRS, EDGE), IEEE 802.11, HIPERLAN/2 and many more.

Protocols according to the different standards are modeled with the help of the *Specification and Description Language* (SDL) [128], a de facto standard for the description of complex workflows in telecommunication. Extensive calculations, e.g., with respect to channel modeling, pathloss and mobility, are implemented using C/C++ code to speed up simulations. Furthermore, dedicated scientific libraries to support stochastic event-driven simulation have been developed at ComNets. The *SDL Performance Evaluation Environment and Tools Class Library* (SPEETCL) is a C++ class library that provides the necessary framework. On the one hand, it supports generation of random numbers with specific distributions to model arbitrary service characteristics (Load Generators); on the other hand, SPEETCL provides means for statistical evaluation. Additional support is given by the automatic code generation tool SDL2SPEETCL that converts syntactically and semantically correct specifications from SDL phrase representation format to C++. Both, SPEETCL and SDL2SPEETCL are part of the professional SPEET environment [131].

The scope of this thesis is to investigate interworking of heterogeneous systems. For this, a joint simulation environment was created, allowing for coincident and parallel operation of actually system specific stand-alone simulators. Important tasks that were implemented in the scope of this work include:

- Time synchronization (common & aligned timing function of different simulation environments)
- Context transfer (queue lengths, buffer states, time stamps of packet generation)
- Overall load generation across simulator namespaces
- Joint evaluation classes (E2E delay performance for VHO)

Main achievement was the design and implementation of the *extended Hybrid Information System* (eHIS) including handover management functionalities and the actual HIS implementation. An overview of the conceptual architecture is given in Figure 7.1.
Figure 7.1: Coupling of Simulation Environments and Extended HIS

The heterogeneous systems that were coupled comprise UMTS and IEEE 802.11. However, the generic design allows incorporation of further specifications as well.

The following chapter describes basic properties and implementation aspects of the stand-alone UMTS simulator URIS and the 802.11 simulator S-WARP. Further, important changes to interconnect eHIS and to allow for heterogeneous system interworking are presented.

7.2 S-WARP

S-WARP (SPEETCL-based Wireless Access Radio Protocol) is an event driven protocol simulator that was developed at the Chair of Communication Networks to simulate different WLAN radio access networks. Initial versions developed by Kadelka [132] and Esseling [133] were used to investigate the HIPERLAN/2 protocol stack. Being based on the same OFDM physical transmission scheme, Mangold [86] has provided a rewrite with standard conform implementation of the legacy IEEE 802.11 protocol. Further enhancements taken up address QoS support with respect to 802.11e.
7.2.1 General Overview

A general overview of the S-WARP simulator structure is given in Figure 7.2. According to the specification, the implementation addresses the lower two layers of the ISO/OSI model. A block \textit{btHigherLayerDummy} models interconnection to layer 3 and above. Evaluations e.g., with respect to throughput are performed on top of layer two. Blocks on the right side of Figure 7.2 take over management functions. While the block \textit{btMLME} is responsible for MAC layer management, the block \textit{btPLME} controls the physical layer. Overall administration is performed by the station management block \textit{btSME}. Blocks on the left side of Figure 7.2 implement the 802.11a,e protocol family. The block \textit{btMPDU\_Generation} receives packets from \textit{btHigherLayerDummy} and manages different priority queues while the block \textit{btProtocol\_Control} manages $T_x/R_x$ coordination, backoff handling and scheduling. Interconnection to channel models implemented in S-GOOSE is realized via the \textit{btPHY} block.

In principle, the number of stations to be simulated is not restricted. The object-oriented approach of the simulator allows for instantiation of any number of stations, each featuring the entire protocol stack. However, focus of this work is on modeling and investigation of single handover events considering a detailed protocol workflow for which the number of users per scenario is rather limited. For scenarios with some hundreds of users, more appropriate system level simulators are available at the Chair of Communication Networks as used by e.g., Kraemling [114].

7.2.2 Specific Changes

Several modifications and enhancements were made in the scope of this thesis to the S-WARP 802.11 protocol simulator including:

- Integration of spectrum management according to 802.11h as described in Section 2.2.5,
- Integration of radio resource measurements according to 802.11k as described Annex C,
- Directed antennas,
- Windowed Link Adaptation mechanisms as described in Section 8.4.1.1
- Multi-Hop packet forwarding,
- Enhanced queue handling (important for VHO in e.g., multihop scenarios),
- Context transfers in terms of queue elements via eHIS as described in Section 7.5.2.1,
- Central mobility control for both, S-WARP and URIS, by S-GOOSE.

Figure 7.2 gives an overview of the S-WARP simulator structure and indicates where the modifications have been implemented.\(^{30}\)

![Figure 7.2: S-WARP Simulator Structure](image)

The block `btHigherLayerInterface` serves as start- and ending point for E2E connections. Additional logic was added to distinguish between one-hop and multi-hop connections. After receiving a packet from `btReception` it is checked whether this packet has been transmitted across all the hops specified for the associated route. If this is true, the packet is passed to another new process for global evaluation. Otherwise, the next hop is retrieved from the route informa-

\(^{30}\) Parts of the discussed items have been jointly specified with [A2] and [A3] within diploma theses under supervision of the author.
tion and the packet is passed on to the \textit{MPDU}Generation block to be transmitted across the next hop.

The block \textit{btMPDU Generation} was modified to enable context transfer, which was not possible with the original S-WARP queue structure. For each traffic category, one separate FIFO queue existed. All \textit{Protocol Data Units} (PDUs) of the same traffic category were put to the same queue, regardless of the destination address. While this works fine for stand-alone 802.11 systems, problems arise if one queue holds packets from several connections respectively stations. If a particular station wants to handover to UMTS, it must be possible to identify and transfer all of its packets that may be split among different priority queues. The new implementation allows for realization of VHO on a connection basis. For each connection (identified by the destination address), the appropriate queue is exported to the eHIS. During context transfers, PDUs are taken from these queues and passed to URIS for transmission in UMTS.

The interface for context transfer and data exchange with the eHIS is realized by the \textit{Station Management Entity} (SME). The SME also handles incoming measurement reports. Mobility support was realized by modifying the SME and the \textit{PHY Layer Management Entity} (PLME) to retrieve the current terminal's position from S-GOOSE. When hybrid mobile terminals leave 802.11, all routes maintained to their communication partners are released. This stops traffic generation and measurement report generation. The communication route is removed from the AP. If a mobile terminal switches to 802.11, all routes are established accordingly. Route establishment and removal is another task controlled by the SME.

\textbf{7.3 URIS}

In order to investigate UMTS communication protocols, a highly sophisticated event driven and modular simulation tool called \textit{UMTS Radio Interface Simulator} (URIS) was applied. URIS has been developed at the Chair of Communication Networks incorporating labor and expertise of many diploma- and PhD theses, e.g., [122]. The focus is on investigations of layer 2 and layer 3 of the corresponding ISO/OSI model though higher layer protocols may be incorporated, too. On top of the protocols, load generators provide traffic according to specific service characteristics.
7.3.1 General Overview

The UMTS protocol stack was formally specified and implemented using SDL. Each *User Equipment* (UE) as well as each *UMTS Terrestrial Radio Access Network* (UTRAN) is represented by one instance of an SDL system, see Figure 7.3. The *User Equipment* encloses SDL specifications of the UMTS layers 2 and 3 as well as higher layer parts (TCP/UDP). All specifications have been implemented on a per bit basis allowing for detailed modeling and accurate performance analysis. The UMTS protocol specification was enhanced by non-standardized but essential algorithms for operation. This comprises *Medium Access Control* (MAC), Scheduling (MAC) and Error Correction (RLC).

The SDL system *UTRA* encloses SDL specifications of the UMTS layers 2 and 3 as well as TCP/UDP parts of layer 4. In addition, Node B and *Radio Network Controller* (RNC) specific functions have been implemented.

In addition to SDL based systems, URIS provides additional functional modules written in C++. They are based on SPEETCL and support load generation, simulation control and statistical evaluation.

![Figure 7.3: Structure of the UMTS Simulator URIS](image)
Since the scope of this work is not on optimizations of the stand-alone UMTS specification, a detailed description of all URIS properties is omitted but can be found in [122]. Instead, functions for interworking with other systems, especially 802.11, are presented. Respective modifications to support intersystem information provisioning and context transfer are described in the following section.

### 7.3.2 URIS Modifications

While Figure 7.3 reflects the overall relation of URIS modules, Figure 7.4 depicts detailed protocol dependencies between the different layers. The shown SDL system represents the functionality of a single UE according to one of the four building blocks on the left side in Figure 7.3. Multiple mobile terminals are simulated by instantiating multiple SDL Systems, one for each mobile, while there is only one SDL System to represent the RNC entity containing all attached NodeBs. For simplification, the transparent mode is used for transmissions in UMTS. This mode does not use any acknowledgments or re-transmissions reflecting the requirements for time-bounded real-time traffic such as voice. Context transfer during vertical handover is realized by exporting the
transmission queue of the RLC transparent mode transmission entity to the Handover Manager of eHIS, see Figure 7.1. When vertical handovers are triggered by HIS, the Handover Manager performs context transfer and redirects packet generation from the old to the new system. For this, respective switches have been added to the URIS SDL Environment.

To evaluate packet delay across system boundaries after VHO, originally generated PDUs of the one system are attached to native PDUs of the other system, thus preserving their time stamp, and transmitted accordingly (for details refer to Section 7.5.2.1). An evaluation block was implemented that is available to both involved systems, URIS and S-WARP. URIS was extended to use this global evaluation for all received PDUs, depacketizing the original PDU if necessary. Similar to S-WARP, evaluation takes place on L2, within the transparent mode reception entity of the RLC Block, as indicated in Figure 7.4.

Measurements gathered from UMTS focus on provisioning of positioning information of mobile terminals to be stored in the Hybrid Information System. HIS polls periodically mobiles’ positions being provided by the S-GOOSE that manages mobility for URIS. The respective points of interest from a system integration point of view in the UMTS simulator are shown in Figure 7.4.

7.4 S-GOOSE/RISE

The scope of S-WARP and URIS is on simulation of communication protocols addressing the logical flow of signals. SDL with its ability to model extended finite state machines hence is an expedient and intuitive programming language to be applied. However, processing intensive tasks should rather be implemented using high-performance programming languages.

Accordingly, channel related calculations have been separated from pure protocol modeling. Pathloss properties, shadowing and fading are challenging tasks for which an implementation in C++ has been favored to speed up simulations. Dedicated interfaces serve as connector between SDL-based protocol simulators and C++ based channel simulators. Interface Data Units (IDU) carrying physical PDUs are passed to the channel model. Transmission related properties such as resulting Carrier-to-Interference Ratio (C/I) are computed and attached to the IDU. The whole packet is then given back to the receiving instance of the protocol simulator that decides for further actions to be taken.
Within this thesis, channel related calculations have been executed by the specific system level simulators S-GOOSE (SDL-Generic Object-Oriented Simulation Environment), respectively RISE (Radio Interference Simulation Engine) came into operation. Both tools have been developed at the Chair of Communication Networks. They comprise experience and expertise from over ten years of research on mobile radio networks.

S-GOOSE originally was developed for interference calculations within GSM/(E)GPRS networks. Within its further development, a rewrite became necessary resulting in a new simulator with enhanced properties referred to as RISE. Compared to S-GOOSE, RISE has been extended to perform much more sophisticated interference calculations, including e.g., multi-cellular scenarios. In addition, WCDMA as applied by UMTS was implemented. Due to its modular approach, different propagation (channel) models may easily be integrated. Current implementations comprise free-space propagation, one-slope model, dual-slope model, Hata-Okumura, Walfish-Ikegami and reference models due to UMTS 30.03 [201]. A good overview of related properties is given by Forkel in [113]. Unless stated otherwise, the vehicular test environment model due to UMTS 30.03 is applied for UMTS simulations. For WLAN, a modified free-space propagation model [157] is applied introducing a pathloss coefficient $\gamma$ that depends on the given surrounding ($\gamma = 2$ $\Rightarrow$ free space, $\gamma = 5$ $\Rightarrow$ high attenuation, e.g., in cities).

7.5 Extended HIS

Chapter 5 introduced the general concept of the Hybrid Information System whose objective is to support interworking between heterogeneous networks by providing cross-system information. Within this work, the raw concept has been developed from its initial stage to a concrete cooperation scheme with prototypical implementation.

Figure 7.1 showed the logical interaction of UMTS, 802.11, and the intermediary Hybrid Information System. HIS itself is embedded in a so called extended HIS (eHIS) environment. This is to indicate that besides the pure monitoring and controlling on the part of HIS, further actions are to be administered, one of which is to accomplish the logical context transfer between the two radio sys-
tems by the so-called *Handover Manager*. Based on triggers from HIS, the handover manager holds responsible for vertical handover control.

Another task of the Handover Manager is to serve as abstraction layer for successful incorporation of several simulators of different communication systems. Each associated simulator needs to implement an interface for communication with the Handover Manager. This allows future integration of additional radio system simulators without significant changes to the actual HIS. HIS interacts solely with the *Handover Manager*.

### 7.5.1 HIS

Figure 7.5 shows a detailed view of the HIS block. Feeding of the Hybrid Information System takes place by measurement reports and/or positioning information. Both may arrive in arbitrary order. To improve accuracy, the erroneous positions are filtered by a position estimator that takes into account the user's movement.

![Figure 7.5: HIS internal setup and decision finding process](image)

**Figure 7.5: HIS internal setup and decision finding process**
Trigger generation takes place either on request (passive/reactive HIS) or autonomously (pro-active HIS). For this, HIS does not check the entire database but evaluates a local link state map. The local map is defined by a Decision Area (DA) around the actual position of a mobile. Hence, only measurement reports that are relevant for a decision are requested from the databases. Measurements taken geographically far away from the mobile’s position have no impact on a decision’s outcome.

Selection of required database entries is taken over by Link Status Aggregation block. The subset of available measurement reports is then processed by a Decision Algorithm that decides for firing of triggers. Additional support by the Position Tracking and Prediction block allows anticipating triggers in the near future. The modular design allows further criteria to be considered by the decision algorithms, such as user QoS/User demands, Joined Radio Resource Management (JRRM) or Load Balancing.

The Hybrid Information System was implemented completely in C++. Interface classes connect the main entities, Decision Unit and the Databases, to the Handover Manager.

Database implementations are based on the open source relational database SQLite [129]. Relying on a file based relational database has several benefits: First, development time is significantly reduced due to application of standardized modules. Second, incorporation of a relational database system into the simulator project allows for early identification of limitations a Hybrid Information System must overcome to be successfully built in reality (with respect to e.g. complexity of entries or data administration). Finally, being a file-based database SQLite allows for data sharing between different simulations for initialization of new setups or derivation of long-term databases by accumulative (parallel simulations) or incremental (consecutive simulations) data collection.

7.5.2 HO Manager

For the investigation of vertical handover between UMTS and WLAN, a simulation environment as shown in Figure 7.6 was created. Multiple mobile stations may be managed by one instance of the Hybrid Information System. To simulate mobile stations equipped with both, the UMTS and IEEE 802.11 protocol stack, two existing protocol simulators were coupled using the Module Loader concept to be described in Section 7.6.1.
A Handover Manager has been defined to manage context transfer and proper handover control. Main task is to abstract from the (implementation dependent) specifics of associated simulators in order to provide a system-independent interface to the Hybrid Information System. Hence, from HIS’ point of view, stations as integrated by the Handover Manager appear as single-device dual mode terminal. Vertical handover may be triggered using one single signal.

---

**Figure 7.6: Extended Hybrid Information System**

### 7.5.2.1 Realization of Vertical Handovers

Vertical handover requires the transfer of queued packets from one system to another. Addressing L2-handover, sophisticated techniques to convert Protocol Data Units (PDUs) between different protocols need to be applied.\(^\text{31}\)

Context transfers between different systems are modeled by transferring queue elements from one simulator to the other. To overcome the problem of adapting

---

\(^{31}\) Scope of this work is on L2 handover. Obviously, it is also possible to apply handover based on higher layers only, e.g., IP Layer handovers without necessity for PDU conversion, discarding all Layer 2 PDUs. However, this may result in time critical necessity for re-transmissions.
PDU formats the simulator generates new native PDUs within the target system with the same length and associates the original PDU with the new one. Figure 7.7 shows this process for a context transfer done during vertical handover from UMTS to 802.11. For each packet in the UMTS transmission queue a new 802.11 packet is created. The object representing this packet has the capability to take a pointer to a foreign packet object. In that way, packets are associated with one another representing the same size while preserving the original generation time stamp. After transmission, packets are passed to a global evaluation instance that accesses the original packet to evaluate throughput and delay.

![Figure 7.7: Context Transfer between UMTS and 802.11](image)

The Handover Manager within the eHIS building block is able to manage multiple mobile terminals. It can be chosen whether a particular station is a dual mode terminal (= support of UMTS & WLAN) or single mode terminal (= support of either UMTS or WLAN). Three types of connections are distinguished:

**Shared:** This connection type is available both, in the UMTS and in the 802.11 simulator. During vertical handover, packets are transferred between the associated queues, i.e. the context transfer as described in Figure 7.7 is triggered. Connections in the old system get deactivated and connections in the new system get activated.

**URIS:** This connection is available in UMTS only. No context transfer is done during handover. Instead this connection is (de)activated. Corresponding queues are not modified.

**S-WARP:** This connection type is identical to the URIS connection type except that it is only available in 802.11.
The introduction of these connection types gives users the opportunity to parameterize sophisticated scenarios. Especially traffic mixes with different services and different QoS demands may be evaluated. It is for example possible to examine scenarios where a mobile terminal moves towards an 802.11 Hot Spot carrying a Voice over IP (VoIP) call in the UMTS system. After VHO, the VoIP call is carried on in the 802.11 cell with high priority while at the same time a low priority FTP file transfer is started as background traffic. It is then possible to evaluate throughput and packet delay for VoIP and FTP separately.

### 7.5.2.1.1 Vertical Handover Procedure

The following subsection describes the procedure executed by the Handover Manager when a vertical handover is triggered by HIS. The considered scenario assumes a mobile terminal that maintains a VoIP service while being connected to UMTS. On moving into the coverage area of a WLAN Hot Spot, the station receives a trigger from HIS to perform a vertical handover. Figure 7.8 presents a Message Sequence Chart (MSC) of the signal flow. On top, the participating entities are shown. The mobile terminal is represented by \textit{STAENT\_VHO}.

The mobile has got one outgoing connection to the NodeB and to the AP in WLAN. This connection entity is represented by the \textit{UPLINK\_VoIP} instance. The instance \textit{STAENT\_AP} represents the combined station entity of NodeB and AP. The downlink connection that is provided by the NodeB while in UMTS and the AP while in WLAN is represented by \textit{Downlink\_VoIP}. The protocol simulators and their interfaces are represented by \textit{URIS} and \textit{S\-WARP} instances.

To initiate a vertical handover towards WLAN, HIS sends the trigger \textit{sHOToW-LAN} to the mobile terminal. This signal is only processed if the mobile terminal is currently in UMTS. The mobile terminal informs all of its associated connections about the handover by forwarding \textit{sHOToWLAN} to each connection entity. In addition, \textit{sVHO\_ind} is sent to the Station Manager to ensure that all downlink connections to the mobile terminal will also be handed over. The \textit{STAENT\_VHO} then changes its state to \textit{WLAN}. Since the uplink connection is of type \textit{SHARED}, it must perform context transfer.
On reception of $s\text{HOToWLAN}$, the connection entity first checks if it is in the $\text{SHAREDUMTS}$ state, otherwise the signal is ignored. Hereafter it starts the WLAN traffic generator and stops packet generation in UMTS. At the same time, communication routes within WLAN are established. Since route establishment within S-WARP requires simulation time to be passed, an infinitesimal short timer $\text{waitDeltaTime}$ is started. When communication routes have been set up successfully, context transfer may begin. For each packet in the associated UMTS queue, the signal $s\text{TransferQueueElement}$ is sent to the S-WARP along with the packet. This creates native 802.11 PDUs with the UMTS PDU being
attached. After queue transfer has finished, the connection entity sets its state to \textit{SHAREDWLAN} to indicate that the VHO for the uplink direction has finished. Upon reception of \textit{sVHO\_ind}, the Station Manager forwards this signal to all known Station Entities. Only Station Entities connected to the backbone network respond to this signal. The \textit{STAENT\_AP} forwards this signal to all its outgoing connection entities. Each of these connections checks whether the destination is the \textit{STAENT\_VHO} and sends the signal \textit{sHOToWLAN} to itself. Context transfer subsequently is performed in the same manner as for the uplink connection.

7.6 Simulator Integration & Modeling

The coupling of different simulators available at ComNets allows for important context transfer between heterogeneous systems. Special attention was put on queue transfer during handover to allow for proper VHO simulations. Thereby, it is possible to distinguish between different traffic classes (TC) so that final E2E performance evaluation is possible. The handover direction is not restricted to a specific scenario so that both ways, upward and downward VHO, are supported. The two-way direction support is of special interest for scenarios, in which a MT traverses a WLAN Hot Spot. In addition to performance evaluation with respect to throughput, further E2E evaluations with respect to E2E delay are possible. This holds for all kinds of packets being

- generated in UMTS & consumed in UMTS  - generated in WLAN & consumed in WLAN
- generated in UMTS & consumed in WLAN  - generated in WLAN & consumed in UMTS

Hence, an arbitrary combination of generating- and consuming system is possible including the case that packets are generated in the one system, handed over to another system and handed over back to the original system (further iterations possible). This is important in case of ping-pong handovers possibly occurring during simulation execution.

7.6.1 Module Loader

Many simulators developed at the Chair of Communication Networks are event driven simulators based on SPEETCL (\textit{SDL Performance Evaluation Environment and Tool Class Library}) providing event schedulers as well as random number generators, random distributions, evaluation classes and container classes. Protocol stacks are specified using the SDL language and are then translated to C++ using the tool SDL2SPEETCL. With all simulators based on SPEETCL, a common platform is provided for integration of actually stand-
alone simulators. The basic idea is to build shared libraries of all simulators one wishes to integrate and to provide a framework, referred to as *Module Loader*, to load these libraries and execute them as a single process.

Figure 7.9: Module Loader Concept

Effective coupling of heterogeneous simulators requires all of them to apply the same time basis. The Module Loader enforces synchronization by providing one single event scheduler among all modules (= libraries/simulators). In addition, random numbers used within the coupled system originate from one single random number generator to avoid correlation between random processes.

### 7.6.2 Combined Statistical Evaluation

All simulation tools include sophisticated statistical evaluation properties applying the probes concept from SPEETCL [131]. SPEETCL probes support both, simple evaluation dumps and statistical reliability based on the Batch Means Algorithms or the discrete *Limited Relative Error* (LRE), respectively. Unless stated otherwise, the LRE algorithm with a maximum relative error of 5 % is applied. For more information on the LRE algorithm, please refer to [134].
The concept has been enhanced to incorporate SQLite [129] database supported evaluation that allows considering time stamp information. Statistical evaluation can be done applying all sophisticated sorting criteria known from similar database engines. Further, this approach allows derivation of initial results even during runtime of the actual simulation. Feeding and reading of values into and from the database are two independent actions that may be performed (quasi) simultaneously.

Packet delay evaluation after vertical handover is only possible if context transfer has been accomplished. In addition, creation timestamps of packets need to be preserved in spite of system interchange. A global evaluation entity has been implemented within the eHIS. The class hoif_evaluation implements the unpack() method that takes either a UMTS PDU or an 802.11 PDU and retrieves the originally generated packet including the time stamp. The original packet is then used by the eval_Objects() method for cross-simulator delay and throughput evaluation. Analysis of results can be done separately for each connection allowing for evaluation of specific traffic mixes.

7.7 Simulator Validation

To allow for investigation of vertical handover and cooperation of heterogeneous RANs, two complex protocol simulators have been modified and enhanced in the scope of this thesis. Both, URIS and S-WARP, originally had been designed for stand-alone operation. In addition, the Hybrid Information System was conceived and implemented to control VHO triggering and context transfer.

Prior to further investigations, it is hence necessary to ensure that the implemented overall simulation environment produces traceable and thus reliable and trustful results. Simple test scenarios that allow for analytical validation have been specified and will be presented in the following.

7.7.1 Queue Transfer

The scenario in Figure 7.10 used to evaluate system performance during VHO is part of the scenario in Figure 6.9. The focus is the transition zone that was referred to by $d_{\text{max}}$. The underlying policy is that the user wants to be handed over to WLAN whenever coverage is given. The required bandwidth is assumed to be 512 kbit/s resembling e.g., a streaming service. WLAN can easily cope with the
requested throughput, but the UMTS radio link has been limited to carry 256 kbit/s only (due to UMTS RRM, interference, user contracts,…). Traversing an area with partial WLAN coverage necessitates a series of upward and downward VHOs to maintain an active session. Elastic buffering as discussed in Section 6.3 is used as complementary proxy management technique while being connected to UMTS.

The following investigations aim at validating the E2E packet delay introduced by VHO and buffering. Evaluation starts right after upward VHO execution from WLAN (AP1) to UMTS (Node B) at $T_{up} = 0$ s. The transmission buffer thus is assumed empty and no queue transfer is necessary. Depending on the terminal’s velocity ($v_1$-$v_5$), it takes a specific amount of time until the coverage area of AP2 is reached. Assuming a fixed distance $d_{max} = 200$ m, $v_1$-$v_5$ directly
correspond to specific amounts of data to be transferred within UMTS during the transition from AP1 to AP2, see Figure 7.10. The reference amount of data for which evaluation is performed is 1MB. If downward VHO from UMTS to WLAN (time: T\textsubscript{down1-5}) is triggered before 1MB of data was transmitted, the remaining amount of data (including packets in the transmission queue) is conveyed across the 802.11 link (AP2).

Figure 7.11 exemplarily depicts throughput and queue length evaluation for a velocity of v\textsubscript{2} = 46 km/h. The downward VHO is triggered at T\textsubscript{down2} = 15.6 s, which means half of the reference data has been transferred via UMTS and the other half via 802.11.

Since the 256 kbit/s RAB in UMTS is not able to convey packets arriving at \( \lambda_{\text{stream}} \) = 512 kbit/s, remaining packets are queued whereas the maximum queue size amounts 2000 packets. Further arriving packets are dropped. When handover is triggered, the queue is transferred to the WLAN system and transmission continues within 802.11.

It is shown in Figure 7.11 that the MT's link to the AP is able to carry much more traffic than the UMTS bearer does. Peak data rates being reached during clearing of the queue achieve approx. 3.5 Mbit/s. Further transmissions take place until the reference amount of data (1MB) has been transferred. The resulting bit rate corresponds to the offered load of 512 kbit/s.

Figure 7.11: Throughput and Queue Length for VHO

\( v_2 = 46 \text{ km/h}, T_{\text{down2}} = 15.6 \text{ s}, \text{ data in UMTS: 500 kB} \)
Figure 7.12 shows the queue length of all simulations ($v_1$-$v_5$) and the corresponding Cumulative Distribution Function (CDF) for the E2E packet delay. The case described before ($v_2$) is included as well. It can be seen from the queue length figure that downward VHO is triggered at different times ($T_{\text{down}1}$-$T_{\text{down}5}$). The course of all queue length plots is very similar. The rising edge is identical being directly related to the difference between offered load and carried traffic within UMTS. A special case holds if VHO is triggered after 320kB have been transmitted ($v_1$). No packets are dropped in that case. The curve parameter is the amount of data transferred within UMTS before VHO is triggered. In the case that all packets are transmitted across the UMTS connection ($v_5$), the queue is filled and is never emptied since no VHO is triggered. As the queue length increases, the delay increases, too.

![Figure 7.12: Queue length & packet delay during VHO for different velocities $v_1$-$v_5$](image)

The waiting time $\tau_W$ for a packet transmitted at time $T$ can be analytically verified by applying models from queuing theory, see Figure 7.13. The investigated case corresponds to a D/G/1-FCFS model using a two-point distribution for the service rate $\mu$. Prior to downward VHO to WLAN, the service rate $\mu$ is limited by the assumed resource limitation in UMTS resulting in $\mu_{\text{UMTS}} \leq 256$ kbit/s. After VHO the service rate $\mu_{\text{WLAN}}$ applies. Since service rates depend on a variety of influencing variables, the distribution of service times is of general nature, indicated by ‘G’ in the Kendall notation. In addition, no simultaneous transmissions in UMTS and WLAN take place and therefore only one active element
applies in the server ‘G/1’. The arrival rate was assumed to be a constant bit rate stream at \( \lambda_{\text{Stream}} = 512 \text{ kbit/s} \) for which a deterministic arrival process ‘D’ is written. Since packets are queued and transmitted according to their order of arrival, the processing strategy is First Come First Serve (FCFS).

Figure 7.13: Classification of VHO as queuing system D/G/1-FCFS

To derive a delay value \( \tau_w \), the following equation needs to be solved:

\[
T \int_{T-\tau_w}^{T} \mu(t) dt = L_Q(T-\tau_w) * P_s \tag{7.1}
\]

\( L_Q \) hereby denotes the queue length given by the scenario parameters \( \lambda \) (arrival rate of packets = load generated by streaming service), \( \mu_{\text{UMTS}} \) and \( \mu_{\text{WLAN}} \) (service rates of UMTS and WLAN), \( T_{\text{down}} \) (time of VHO from UMTS to WLAN). \( T_{\text{Qfull}} \) (time when queue reaches \( L_{Q\text{max}} \)) and \( T_{\text{Qempty}} \) (time when the queue is processed after VHO) are a function of the maximum queue size \( L_{Q\text{max}} \) and the arrival and service rates. \( P_s \) represents the chosen packet size. Assuming no initial queue at simulation start \( (L_Q(0) = 0) \), \( L_Q(t) \) is given by:

\[
L_Q(t) * P_s = \begin{cases} 
(\lambda - \mu_{\text{UMTS}}) * t & \text{if } t < T_{\text{Qfull}} \\
L_{Q\text{max}} * P_s & \text{if } T_{\text{Qfull}} \leq t < T_{\text{VHO\text{down}}} \\
L_{Q\text{max}} * P_s - (\mu_{\text{WLAN}} - \lambda)(t - T_{\text{VHO}}) & \text{if } T_{\text{VHO\text{down}}} \leq t < T_{\text{Qempty}} \\
0 & \text{if } t \geq T_{\text{Qempty}}
\end{cases} \tag{7.2}
\]

Equation (7.1) cannot be solved for all time instances easily. Nevertheless, significant points in the delay distribution of Figure 7.12 can be verified.
Example 1: Determination of maximum delay $\tau_{W_{\text{max}}}$:
The maximum delay in Figure 7.12 is $\tau_{W_{\text{max}}} = 10$ s. These are packets occupying the last slot in the queue and are transferred solely within UMTS prior to VHO to WLAN. Therefore $L_Q(t) = L_{Q_{\text{max}}}$ and $\mu(t) = \mu_{\text{UMTS}} = \text{const}$, so that (7.1) becomes:

$$\tau_{W_{\text{max}}} = \frac{L_{Q_{\text{max}}} * P_s}{\mu_{\text{UMTS}}} = \frac{2000 * 160 \text{ byte}}{256 \text{ kbit/s}} = 10 \text{ s}$$  \hspace{1cm} (7.3)

Higher delays than $\tau_{W_{\text{max}}}$ are not possible since packets arriving when the transmission queue is full are discarded.

Example 2: Determination of characteristic kink for $v_4$:
In case that VHO is triggered after 773 kB ($v_4 = 30$ km/h, $T_{\text{down}4} = 24.2$ s) have been transmitted within UMTS a remaining data volume of 227 kB is transferred within WLAN. Keeping in mind that the assumed queue consists of 2000 packets, each carrying 160 bytes, results in 320 kB that are transferred during hand-over from UMTS to WLAN for subsequent transmission.

Figure 7.12 shows that the queue is completely filled when downward VHO is triggered. This means, that none of the packets that arrive after VHO execution are of interest for the delay evaluation since it was claimed that simulation stops after an E2E transfer of 1MB. Therefore, the last packet that is evaluated is transmitted after:

$$T = T_{VHO} + \frac{227 \text{kByte}}{\mu_{\text{WLAN}}} = T_{VHO} + 0.52s$$ \hspace{1cm} (7.4)

All packets that are conveyed by WLAN originate from UMTS, for which $T - \tau_W \leq T_{VHO}$. Solving (7.1) for these boundary conditions gives:

$$\tau_w = \frac{L_{Q_{\text{max}}}}{\mu_{\text{UMTS}}} - (\frac{\mu_{\text{WLAN}}}{\mu_{\text{UMTS}}} - 1)(T - T_{VHO})$$ \hspace{1cm} (7.5)

Evaluation for the last packet transmitted after VHO while considering (7.4) results to $\tau_{W1} = 3.41$ s which corresponds to the characteristic kink for $v_4$ in Figure 7.12. This explains the increased probability of packets with a delay between $\tau_{W1}$ and $\tau_{W_{\text{max}}}$ for the packet delay curve when VHO is triggered after 773 kB have been transferred.
In a similar approach, other significant delay values may be verified. Early triggering of VHO due to increased terminal velocity \((v_1 > v_2 > \ldots > v_5)\) results in more and more packets being directly transferred within WLAN and thus without previous waiting in the queue. Transmission delay within WLAN is very low, so these delay values cause an initial saltus \((\text{saltus } 1 > \text{saltus } 2 > \text{saltus } 3)\) in the packet delay CDF.

### 7.7.2 RPI Measurements

Vertical handover control by the Hybrid Information System is based on exploitation of measurements being stored in the database. In addition to the more general *Basic Report*, IEEE 802.11h defines two further fundamental measurement reports, the *Clear Channel Assessment Report* and the *RPI Histogram Report*, cp. Section 2.2.5. Both kinds of reports have been implemented in the scope of this thesis. Since (downward) VHO decisions in large parts depend on this information, the following section targets on validation of WLAN measurement reports as provided by feeding clients.

A simple scenario according to Figure 7.14 was chosen, within which a station approaches the coverage area of an access point. As soon as it enters the Hot Spot, a VHO trigger is fired by HIS and the station performs downward VHO to WLAN. After association, a bidirectional symmetric connection is established with offered load of 256 kbit/s (a), 1000 kbit/s (b) or 3000 kbit/s (c, d). While for the first two load conditions, a fixed PHY-Mode of BPSK \(\frac{1}{2}\) supporting data rates up to 6 Mbit/s was chosen, scenario (c, d) applies *Link Adaptation* (LA). During the entire connection, both, AP and the station perform measurements in intervals of 200 ms. Transportation of MRs from the station to the AP are accomplished in a piggybacked manner together with user data.
Figure 7.14: Validation of measurements according to 802.11h
Figure 7.14 a) shows measurements on the downlink as gathered by the mobile terminal. IEEE 802.11h specifies a quantized way to report link qualities by defining so called Received Power Indicator (RPI) levels, see Section 2.2.5.3. Increased reception power is indicated by an increased RPI level. Initial measurement reports are available for distances below 191 m, right after VHO. Distances above 191 m correspond to RPI 1 and are below the minimum required reception threshold of 802.11, see Section 8.3.1.1. For distances between approximately 191 - 120 m, two RPI levels are reported: RPI 0 and RPI 2. While RPI 2 indicates incoming transmissions from the AP, RPI 0 reflects measured receive power levels when no transmission takes place, hence background noise. Accordingly, the fractional part of RPI 0 within the overall measurement duration is a good indicator to estimate the occupancy of the channel. However, since RPI levels can only be measured while sensing the medium, respective reports do not consider channel occupancy due to own transmissions. This is why 802.11h has further specified the ClearChannelAssessment Report with a CCA_BUSY_FRACTION indicator as introduced in Section 2.2.5.2. Nonetheless, similar information can be derived by combining RPI histogram reports gained from both, uplink and downlink measurements. Considering further that a station is aware of its own activities, RPI histograms could be adjusted to indicate own transmissions as well (not foreseen by the specification so far). Hence, all information necessary to derive trigger generation for VHO inherently is entailed in RPI histogram reports (from up- and downlink), for which CCA reports will not explicitly be considered further.

Interpreting RPI 0 as background noise, this means that the channel of the scenario in Figure 7.14 a) is idle for 91 % of the time. This in turn means that the fractional part of RPI 2 in Figure 7.14 a) indicates channel activity at this level of approximately 9 %. Considering that for a given packet size of 160 Byte the maximum throughput to be achieved at BPSK ½ saturates at 2800 kbit/s (cp. Section 8.5.1.1 for further explanations on saturation throughput), this fits well with the fraction of bandwidth occupied by downlink transmissions (256 kbit/s). Reported measurements by the station hence match with expected values. With decreasing distance between station and AP, link quality improves for which

---

32 Due to definition, RPI 2 does not represent receive power from any particular transmission but the accumulation of signal energy during the measurement duration, obviously including background noise. Due to differences in the order of decades, background noise is neglected here and all measured power is considered signal power.
higher RPI levels are reported. Since the PHY-Mode is fixed (BPSK $\frac{1}{2}$) and the load remains the same, no further changes with respect to the RPI X/RPI 0 ratio adjust.

For the scenario in Figure 7.14 b), the offered load was increased to 1000 kbit/s. Since the same fixed PHY-Mode of BPSK $\frac{1}{2}$ is chosen, the expected channel occupancy is presumed to rise due to increased load. Approaching the Hot Spot, the station is triggered to handover at $d = 191$ m. Compared to a), the fractional part of RPI 0 has decreased to 65 %, while the one of RPI 2 has increased to 35 %. Relating this value to the saturation throughput results to $35\% \times \frac{2800}{980} = 980 \text{kbit/s}$, which reflects well the offered load. Approaching further the AP, reported RPI levels increase. Due to fixed PHY-Mode and constant load, no further changes with respect to the RPI X/RPI 0 ratio adjust.

For the scenario according to Figure 7.14 c), the offered load was further increased to 3 Mbit/s. In addition, link adaptation was allowed to select higher PHY-Modes than BPSK $\frac{1}{2}$. On approaching the cell border, the station is triggered to perform VHO. Similar to a) and b), reception at RPI 2 and RPI 0 initially is reported. Due to further increased load, the fraction of RPI 2 is now spanning up to 80 % of channel capacity. This time however, there is no straightforward partitioning between RPI 2 and RPI 0. The reason for this is LA. Based on a simple window mechanism, LA switches to a higher PHY-Mode after consecutive successful reception of $\text{txSucceedRespondValue}$ number of frames. Contrary to this, LA switches to a lower PHY-Mode after consecutive reception of $\text{nAckRespondValue}$ number of non-successful transmissions. Both parameters are adaptively adjusted during simulation. A more detailed description of the applied algorithm is provided in Section 8.4.1.1.

Once LA has chosen a higher PHY-Mode, two states are possible: Either, transmissions are successful ($\Rightarrow$ decreasing RPI 2 ratio) or, due to application of a less robust PHY-Mode, transmission errors occur resulting in re-transmissions adding further load ($\Rightarrow$ increasing RPI 2 ratio) to the system. The latter effect usually applies in conjunction with switching back to a lower PHY-Mode.

As a general observation, one can state for Figure 7.14 c) that channel occupancy decreases with decreasing distance $d$. In other words, the fraction of RPI 0 being reported by the mobile increases and the fractions of RPI X decrease. Reported values match expectations, since the offered load is constant and higher PHY-Modes allow for transfer of more data within less time than lower PHY-
Modes. For distances \(d < 30\, \text{m}\), an almost straightforward ratio of RPI 6/RPI 0, respectively RPI 7/RPI 0, adjusts as already known from Figure 7.14 a) and b). This is due to the fact, that reception quality at RPI 6 and RPI 7 is so good that no transmission errors occur in spite of using the highest PHY-Mode 64 QAM \(\frac{3}{4}\) and hence LA does not switch to lower PHY-Modes again\(^{33}\). The resulting fraction of RPI 7 (and RPI 6) in Figure 7.14 c) denotes approximately 10 %. With a saturation throughput of 30 Mbit/s (64 QAM \(\frac{3}{4}\), 160 byte packet size), this fits fairly well the offered load of 3 Mbit/s.

Finally yet importantly, Figure 7.14 d) depicts complementary measurement reports to c), this time recorded by the AP (uplink) and not by the station (downlink). In general, the same observations as for c) apply. The only difference is that the AP also disposes of MR for \(d > 191\, \text{m}\). While being out of coverage, the mobile is not able to provide any MR at all for which there are no entries for distances \(d > 191\, \text{m}\) in Figure 7.14 a) - c). This in turn means that the AP does not detect any transmissions, for which background noise (RPI 0) is reported.

As a summary, the previous investigations have shown that measurement results according to IEEE 802.11h as implemented and reported in the simulation environment are correct with respect to both, RPI classification and fractional part of channel occupation. The latter was also cross-checked with expected values derived from analysis when considering the given packet size and the theoretical saturation throughput. The verified measurement results hence provide a reliable and trustful basis on which the Hybrid Information System will run appropriate VHO trigger algorithms.

\(^{33}\) Please be aware that all colors in Figure 7.14 refer to measured RPI levels and \textit{not} to the currently applied PHY-Mode! If a station reports that a better RPI level has been measured due to decreased distance, this does not necessarily mean that a better PHY-Mode can be applied!
7. Integrated Simulation Environment
CHAPTER 8

Performance Evaluation

Content

8.1 Services & Scenarios ................................................................. 222
8.2 Detrimental Scanning Impact .................................................... 223
8.3 Enhanced Coverage Detection .................................................. 236
8.4 Context Provisioning ............................................................... 252
8.5 Adaptive Beacon Control ....................................................... 262

Keywords: Scanning Drawbacks, System Detection, Compressed Mode, PHY-Mode Recommendation, Coverage Optimization, Capacity Exploitation, Beacon Management

The following chapter provides simulation results revealing benefits of system control with the Hybrid Information System. First, some general assumptions on simulation scenarios and parameters are presented. Hereafter, drawbacks of conventional system control approaches based on self-conducted scanning are disclosed. For UMTS, it is shown that application of the compressed mode entails drawbacks with respect to system performance. For WLAN, self-conducted scanning results in reduced overall throughput due to delayed hot spot detection. HIS based system control overcomes both of these detriments. Furthermore, a new mechanism for coverage detection is introduced that allows HIS to fire handover triggers in a most optimized way. Additional benefit results from context information to be provided by HIS together with triggers. This is how link adaptation can be anticipated and accelerated. Finally, another example for HIS based system control is presented within which beaconing is beneficially adjusted for the sake of both, a single terminal as well as the entire system. Particular benefit is given for joint application with directed antennas. The resulting use cases disclose a huge potential and would not be feasible without intervention of a sophisticated control logic such as HIS.
8.1 Services & Scenarios

Focus of this work is put on two main goals to be achieved: Sophisticated network selection according to the ABC rule (a service should be handled by/handed over to the most suitable system) and seamless continuity of selected services across network boundaries. Both of these aspects are addressed by the Hybrid Information System.

Support for ABC for a required service is given in the sense that HIS disposes of information with respect to general service support and current network availability. Boundary conditions to be considered comprise predefined user policies but also operator viewpoints. Within an integrated system environment, service dependent network selection will play an increasingly important role. Reasons for which one or another system should be chosen are manifold and have been discussed in Section 3.4. Particular problems arise if ongoing communication relations are given, e.g., a user requests a high-speed download service while doing a voice call. Since high-speed download might not be supported by the current network, another technology will be recommended – if generally and currently available. Since the user does not want to interrupt the voice call, seamless continuity across network boundaries is important. Vertical handover is one means to achieve this goal, fast re-establishment schemes allowing for disassociation in the one system with quasi-parallel association in the other system is another. The Hybrid Information System is the controlling entity in both cases. While backbone signaling for e.g., pre-authentication is out of scope of this thesis, control information to be transmitted via the air-interface is of particular interest.

Unless stated otherwise, the simulations in this section consider interactive real-time-services such as speech or video-telephony as application examples of services with moderate bandwidth- but restrictive delay requirements. In addition, streaming or best-effort data delivery is considered to investigate throughput performance of integrated system control by HIS. Traffic characteristics of related services have been compiled in Table 8.1.
8.2. Detrimental Scanning Impact

Table 8.1: Traffic characteristics and QoS parameters for different services

<table>
<thead>
<tr>
<th>Application</th>
<th>Device</th>
<th>Throughput</th>
<th>Packet size</th>
<th>PER</th>
<th>Delay</th>
<th>Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video conference</td>
<td>AV/Display</td>
<td>128 kbit/s – 2 Mbit/s</td>
<td>Variable ~ 512 B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDA</td>
<td></td>
<td>G.723.1: 24 B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Projector</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice Handset</td>
<td>20 kbit/s – 150 kbit/s</td>
<td>200 byte</td>
<td>5%</td>
<td>30 ms</td>
<td>15 ms</td>
</tr>
<tr>
<td></td>
<td>Laptop/Desktop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP3 Audio</td>
<td>MP3 Player</td>
<td>64 kbit/s – 320 kbit/s</td>
<td>Variable ~ 418 byte</td>
<td>10^-4</td>
<td>200 ms</td>
<td>100 ms</td>
</tr>
<tr>
<td></td>
<td>PDA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Laptop/Desktop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Transfers</td>
<td>Laptop/Desktop</td>
<td>1 Mbit/s</td>
<td>Variable ~300 byte</td>
<td>--</td>
<td>60 s</td>
<td>--</td>
</tr>
<tr>
<td>(email, Web, Chat)</td>
<td>PDA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

8.2 Detrimental Scanning Impact

Vertical handover decision taking needs to resolve preconditions prior to triggering any system change. Obtaining answers to each of the following three questions thereby is essential for successful VHO execution:

1) Existence of a complementary system → “Is there any other system at all”?
2) Service Support → “Does the other system generally support my required service?”
3) Availability → “Is the other system currently able to accept further connections?”

In principle, the listed questions are not restricted to VHO and need to be answered for horizontal handover as well. However, it is the distinct property of VHO to switch to a system with different characteristics, for which especially the aspect of Service Support by a possible handover candidate system is of particular interest.
However, prior to taking (V)HO decisions, knowledge on the existence of a complementary system needs to be present first. Initial approaches for enhanced information provisioning on neighboring systems start finding their way into new specifications; compare Section 3.2.1 on RAN cooperation. However, there are many reasons for which these procedures cannot or shall not be applied, e.g., limitations in the specification (WLAN 802.11 does not offer any means to report on vertical systems), prevention of additional over-the-air overhead in densely loaded scenarios or backwards compatibility with other (older) devices in the networks.

In fact, self-conducted scanning currently is the most important means designed to achieve information on the existence of complementary systems. In addition, the option for self-conducted scanning will always be substantial part of each multi-mode station to be applied as fallback solution if no further information source is available.

While the technical description of scanning procedures as defined for UMTS and WLAN 802.11 was presented in Sections 2.1 and 2.2, the following investigations aim at illustrating some of the negative consequences deriving from scanning. It will be shown, that scanning entails disadvantages for both, a single connection as well as for the entire system.

### 8.2.1 WLAN: System Detection

The following section shall point out negative impacts due to self-conducted scanning. A scenario according to Figure 8.1 is assumed within which a vehicle moves along the street. Full coverage with respect to a cellular system is presumed, while only partial Hot Spot coverage is offered. Due to aspired large file transfers, the user demands for connectivity to WLAN whenever possible. Since no information on Hot Spot deployments is available, the only way for heterogeneous system detection is given by means of self-conducted scanning.

Parameters for the simulation have been user velocity ($v = 3, 7, 14 \text{ m/s}$) and scanning interval ($T_s = 0.1, 0.5, 1.0, 2.0, 3.0, 4.0, 6.0 \text{ s}$), whereby the latter refers to the time span between two subsequent scanning actions. The initial settlement of the car, respectively the time of first measurement, is randomly chosen which is particularly important for high velocities and large scanning intervals. Evaluation metric is the distance $D$ after a reference handover point where detection of
WLAN coverage takes place. The reference HO point is a theoretical boundary defined by receiver sensitivities according to IEEE 802.11. Further investigations on this boundary together with proposals for optimized detection will be given in Section 8.3.1.1. Repetitive simulations runs have been executed to derive distribution functions for $D$ as shown in Figure 8.1 a) – c) until stochastic reliability according to parameters as described in Section 7.6.2 was ensured. The applied beacon interval is assumed sufficiently short and transmissions are error-free, so that scanning inside the Hot Spot area effectively allows for WLAN detection.

Figure 8.1: System detection for different scanning intervals and velocities

In fact, performance of scanning based WLAN detection decreases with increasing velocity. Comparing figures a) – c), this is expressed by a right-shift of curves involving a less steep gradient. Reaching the 100 % ceiling, WLAN detection has successfully completed in all cases. Considering e.g., a velocity of $v = 3$ m/s and a scanning interval of $T_s = 6$ s in a), WLAN is undoubtfully detected for distances $D = 18$ m. This can be simply verified with a ‘worst case’ estimation: Assuming scanning is scheduled \textit{shortly before} entering the Hot
Spot, no detection takes place and another scanning interval elapses prior to next scanning. Meanwhile, the terminal moves

\[ D = \Delta s = v \cdot T_s = 3 \text{ m/s} \cdot 6 \text{ s} = 18 \text{ m}, \]

which matches exactly the 100 %-quantile in Figure 8.1 a).

The second dependency obviously is given by the applied scanning interval \( T_s \). Naturally, detection of WLAN is delayed for increased scanning intervals. Particular attention should be paid for large scanning intervals applied at high velocities: It is shown for \( v = 14 \text{ m/s} \) and \( T_s = 6 \text{ s} \) in Figure 8.1 c), that the CDF saturates at 90 %. The accompanying distance corresponds to 74.6 m corresponding to the diameter of the coverage area\(^3\). This in turn means that 10 % of the users did not detect the WLAN at all.

Investigations in this section have shown that self-conducted scanning should be applied on a periodical basis with minimal possible time span between two subsequent scanning intervals. Considering potential saturation throughputs offered by WLAN comprising up to 35 Mbit/s, it is obvious that large scanning intervals inherently increase the risk for suboptimal performance in terms of throughput. In addition, it is to say that investigations in this section assume coincidence of beacon transmission with scanning as well as error-free reception. Hence, less opportunistic assumptions will further decrease performance of self-conducted scanning.

While it is said and derived from Figure 8.1 that application of decreased scanning intervals is beneficial, this solution is only partly applicable in life networks. Reasons for this are manifold and comprise aspects like power consumption, signaling overhead (with active scanning) and possible delay enhancements. Hence, the fact that scanning of a complementary system may harmfully influence the current system’s performance is another drawback that argues against small scanning intervals.

\[^3\] The resulting coverage is due to the chosen combination of transmission power and pathloss properties. Actual values may be larger or smaller.
This holds in particular, if ongoing connections are maintained, since detection of another heterogeneous system by means of scanning shall not affect current transmissions. The following section particularly addresses problems arising within UMTS-FDD due to scanning of complementary systems.

### 8.2.2 UMTS: Impact of Compressed Mode

The continuous transmission and reception scheme of UTRA-FDD entails problems if measurements of other systems shall be made. The standard considers this by specifying three different transmission time reduction methods, 1) puncturing, 2) higher layer scheduling and 3) reduction of the spreading factor, whose application result in generation of idle slots, so called transmission gaps. All three methods aim at ‘compressing’ data, to allow for quasi-continuous operation. Accordingly, the notation *Compressed Mode* (CM) is used. A detailed CM description has been provided in Section 2.1.3.

However, the different CM methods entail certain drawbacks: Puncturing is only specified for downlink transmission, higher layer scheduling is mainly applicable to packet data with tolerant delay requirements and reduction of the spreading factor requires increased transmission power. Since UMTS is an interference-limited CDMA system, especially the last CM method shall be further discussed. In the following, the influence of compressing data on the overall interference situation is investigated. However, the focus of this thesis is not on CM investigation for which the following simulation scenarios entail some simplifications to allow for less complex environments with decreased simulation efforts. The aim is to illustrate the harmful consequences of CM application rather than deriving performance figures for e.g., definition of dimensioning rules.

\[
\frac{E_b}{N_0} = \frac{S}{N} \times \frac{B}{R} = \frac{S}{N} \times G_p; \quad \text{with} \quad G_p = SF
\]  

(8.2)

An important value for the resulting Bit Error Rate (BER) of a connection is the ratio of $E_b/N_0$, see equation (8.2) [124]. $E_b$ is the Energy per Bit, $N_0$ is the Spectral Noise Density, $S$ and $N$ are carrier signal and background noise, $B$ is the user bandwidth (= chip rate) and $R$ is the data rate (= bit rate). The amount by which the power density of the carrier signal is increased in the receiver is called processing gain $G_p$. The value of the processing gain corresponds to the spreading factor SF and hence to the number of transmitted chips per bit $B/R$. One can see
that in CDMA systems, the $E_b/N_0$ is typically larger than the S/N by the amount of the spreading factor SF.

Accordingly, if the same BER is to be achieved with CM method 3 (reduction of the SF by a factor of 2), this requires transmission power raise of the same amount of +3 dB. Applying compression thus has a direct impact on other transmissions, since the overall interference in a cell is affected. Power control as applied by other devices for compensation will further contribute to an increased overall system interference level.

![Figure 8.2: Simulation scenario for compressed mode analysis](image)

**8.2.2.1 Single Cell Impact**

Within the following, a special focus is put on DL interference. To estimate the influence of CM on the overall DL interference, a single cell with an omnipresent interference level (background noise) $I_0$ being varied between $-80$ dBm $\leq I_0 \leq -100$ dBm is considered. The scenario is used to investigate basic impacts of compressed mode application on the interference level within a cell. More complex effects considering neighbor cell influences and power control are excluded here but will be addressed in Section 8.2.2.2.

The scenario consists of two mobiles $M_{TA,B}$ and one Node B/Base Station (BS) as depicted in Figure 8.2. Since $MT_A$ demands for idle periods to perform scanning, the supplying base station applies CM and thus increases temporarily the transmission power for connection $A$, see Figure 8.2. Due to CDMA inherent parallel downlink transmission from the BS to the terminals, the BS appears as origin of both, carrier signal and interference source at the same time. Regular
transmissions for connection B therefore face an increased interference level. For this, MT_B in the following is considered as victim of CM application for connection A and the base station is referred to as (intra-cell) interferer. The cognition that MT_B faces increased interference is not automatically tantamount to increased BER. The latter depends on the orthogonality properties of the signals that will be taken into account later on.

The path loss model for this scenario is the one for the vehicular test environment as specified within UMTS 30.03 [201],

\[
L(R) = 128.1 + 37.6 \log_2(R) \text{ [dB]}, \quad (8.3)
\]

where \( R \) is the distance between victim and interferer in km and \( L \) is the resulting path loss in dB.

The interfering connection A initially has a fixed transmission power of \( P_{TxNorm} = -10 \text{ dBm} \) (0.1 mW). Afterwards the interferer (BS) raises its transmission power by 3 dB to \( P_{TxCM} = -7 \text{ dBm} \) (0.2 mW) to allow for CM transmission with reduced spreading factor for connection A. The subsequent measured interference \( I_{CM} \) at MT_B after increasing the transmission power

\[
I_{CM}(R) = 10 \cdot \log\left\{ 10^{I_0/10} + (1-\nu) \cdot 10^{[P_{TxCM}-L(R)]/10} \right\} \quad (8.4)
\]

is compared to the interference \( I_{Norm} \) while being in normal mode of operation

\[
I_{Norm}(R) = 10 \cdot \log\left\{ 10^{I_0/10} + (1-\nu) \cdot 10^{[P_{TxNorm}-L(R)]/10} \right\}. \quad (8.5)
\]

Parallel DL transmissions in UMTS ideally do not interfere with each other. Signal spreading with orthogonal codes allows for separation of different user signals in the receiver. However, perfect orthogonality is usually not the case. For this, an orthogonality factor \( \nu \) is introduced which represents a fraction of the received power on the downlink that is seen as intracell-interference by each of the codes from the same BS. The orthogonality factor \( \nu \) accounts for imperfections in orthogonality among signature sequences due to multipath propagation [135]. Equations (8.4) and (8.5) consider this by introducing an orthogonality factor \( \nu \) with \( 0 \leq \nu \leq 1 \). For \( \nu = 1 \), signals are perfectly orthogonal and no cross talking between code channels takes place. Depending on the environment inherent delay spread, the orthogonality factor typically lies between 0.4 and 0.9
For the following investigation, an average orthogonality factor of \( \nu = 0.7 \) was assumed.

Figure 8.3: Interference increase due to DL Compressed Mode application

Figure 8.3 shows the interference deviation \( I_{CM} - I_{Norm} \) as noticed by \( MT_B \) for scenarios with and without compressed mode application. The curves show that \( MT_B \) permanently suffers from a more or less increased interference level. Parameters that were varied are the distance \( R \) between Node B and \( MT_B \) and the omnipresent background noise \( I_o \).

Two effects can be noticed: For a constant omnipresent background noise \( I_o \), the impact of CM application on the noticed interference level at \( MT_B \) decreases with increasing distance \( R \). Moreover, one can see that the impact of the CM decreases with rising background noise. The latter is because the fractal part of the overall interference caused by application of the CM is outweighed by the influence of the background noise.

Based on the given results one can conclude that CM application the more negatively affects the closer an interfered terminal \( MT_B \) resides to the base station. Since Node B acts as both, signal- and interference source for \( MT_B \), the actual
location of MT_A has an indirect influence only. Approaching the cell edge, MT_A terminals are much more likely to request for transmission gaps for scanning than MT_A terminals that are well provided in the centre of a cell. The direct response to one of the requests then is the application of CM by the base station, leading to the previously explained negative impacts on MT_B.

Figure 8.3 shows that, depending on the background noise, the noticed interference increase for a distance of e.g., R = 20 m denotes 2-3 dB, which means that the influence of the CM cannot be neglected.

8.2.2.2 Multi Cell Impact

For the previous investigations in Section 8.2.2.1, only one mobile applying CM was considered. The load in a cell was modeled by varying the background noise. However, an important aspect when it comes to interference calculations is power control in UMTS. Hence, to estimate the impact on the overall interference in a cell or respectively the DL transmission power, power control has to be taken into account.

Figure 8.4: Simulation Scenario with evaluated- and eight interfering cells

Figure 8.4 depicts the respective scenario with an UMTS cell of 350x350 m² in its centre. The cell is uniformly loaded with 48 mobiles, e.g., mobiles are uniformly distributed, resulting in an equidistant spacing between a mobile and its
closest neighbor of 50 m. Inter-cell interference is considered by simulating eight surrounding cells with identical cell dimensions. Only continuous speech transmissions in DL are regarded for which a C/I target of -18 dB \[138\] at the mobiles is to be adjusted. Since especially the feedback of power control on the varying interference is to be investigated, no mobility is applied in this scenario. Table 8.2 summarizes the applied settings.

**Table 8.2: Parameter settings for CM scenario**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario size</td>
<td>1050 m</td>
</tr>
<tr>
<td>Cell size</td>
<td>350 m</td>
</tr>
<tr>
<td>Distance between mobiles</td>
<td>50 m</td>
</tr>
<tr>
<td>Duration Phase 1 (no CM)</td>
<td>500 frames</td>
</tr>
<tr>
<td>Duration Phase 2 (with CM)</td>
<td>10000 frames</td>
</tr>
<tr>
<td>Max. (\text{T}_\text{x}) power</td>
<td>20 dBm</td>
</tr>
<tr>
<td>Target C/I</td>
<td>-18 dB</td>
</tr>
<tr>
<td>Background noise</td>
<td>-103 dBm</td>
</tr>
<tr>
<td>Power control interval</td>
<td>1 per slot (10/15 ms)</td>
</tr>
<tr>
<td>Power raise due to CM</td>
<td>3 dB</td>
</tr>
<tr>
<td>Orthogonality factor</td>
<td>0.4</td>
</tr>
<tr>
<td>Transmission gap length</td>
<td>7 slots</td>
</tr>
<tr>
<td>Transmission gap pattern</td>
<td>slots 0-6, 4-10 and 8-14 (randomly chosen)</td>
</tr>
<tr>
<td>Space between CM frames</td>
<td>2, 3, 5, 10 frames</td>
</tr>
</tbody>
</table>

The simulation is split into two phases. Within the first phase, no CM is applied for which the mobiles will end up in a stable \(\text{T}_\text{x}\) power equilibrium. In phase two, CM is applied to generate a 7 slot transmission gap every 10 (5, 3, 2) radio frames resulting in a CM rate of \(f_{\text{CM}} = 10\) Hz (20 Hz, 33 Hz, 50 Hz). It is calculated as:

\[
f_{\text{CM}} = \frac{N_{\text{CM}}}{N_{\text{total}}} \times \frac{1}{T_{\text{frame}}}, \quad \text{with} \quad N_{\text{CM}} = \text{Number of CM-Frames}
\[
N_{\text{total}} = \text{Total Number of Frames}
\]

If, for example, the CM is applied once \(N_{\text{CM}} = 1\) every 5 frames \(N_{\text{total}} = 5\), the respective CM rate is
From the user point of view, the CM rate denotes how many times per second the base station switches to CM for a particular connection. Assuming an adequate high number of users with non-correlated scanning requests and uniform distribution of CM rates, $f_{CM}$ from the overall system point of view denotes the percentage of connections for which CM is applied simultaneously. Since CM application means increased transmission power of 3 dB around the gap, cp Section 2.1.3, its usage consequently will have an impact on the overall DL transmission power and hence on the intra-system interference, as explained in the previous section.

**Figure 8.5: Power deviation due to CM application**

Figure 8.5 depicts the cumulative distribution function (CDF) of the difference of the overall transmission power in DL with and without CM for varying $f_{CM}$. The CDF is plotted from -0.5 dB to 2.5 dB, however, a minimum deviation of -0.62 dB and a maximum deviation of 3.34 dB were even evaluated, see Table 1,
though with very rare occurrences. The mean deviation computes between 0.36 dB and 1.37 dB, depending on how frequently the CM is used. As a result, the mean interference in a cell will rise by the same amount if CM operation is applied. Note, that due to the nature of code division multiplex, the increase of DL transmission power for a certain connection directly affects interference as seen by other connections, for which these terms have been used synonymously in this context.

Table 8.3: Characteristic values if CM is introduced

<table>
<thead>
<tr>
<th>f_{CM}</th>
<th>Mean deviation</th>
<th>Min deviation</th>
<th>Max deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Hz</td>
<td>0.36 dB</td>
<td>-0.54 dB</td>
<td>2.55 dB</td>
</tr>
<tr>
<td>20 Hz</td>
<td>0.66 dB</td>
<td>-0.62 dB</td>
<td>2.68 dB</td>
</tr>
<tr>
<td>33 Hz</td>
<td>1.06 dB</td>
<td>-0.49 dB</td>
<td>3.27 dB</td>
</tr>
<tr>
<td>50 Hz</td>
<td>1.37 dB</td>
<td>-0.61 dB</td>
<td>3.34 dB</td>
</tr>
</tbody>
</table>

The results indicate that depending on the variation of f_{CM}, up to 10 % of the time the CM may even have a positive impact on the overall interference within the scenario, see Figure 8.5. This is because other links inherently benefit by the transmission gaps introduced due to CM application. Nevertheless, for at least more than 90 % of the time, the overall interference gets worse.

Another important fact is, that though the percentage fraction of deviation values above 0.75 dB amounts less than 10 % for f_{CM} = 10 Hz (whereby this fraction increases to 90 % for higher values of f_{CM}), this impact cannot be neglected due to interference reasons. In addition and even more problematic is the fact that for proper operation respective power control headroom (= fast fading margin) corresponding to the maximum interference increase needs to be reserved for the terminals. In the scenario as examined here, this would correspond to a maximum value of 3.34 dB in order to serve all mobiles. This in turn means that the cell coverage is reduced by the same amount or that the mobiles need a link-margin that is increased by approximately the respective maximum deviation.

Accordingly, one can say that CM as a means to allow for scanning other systems features by some positive and a number of negative aspects as listed in the following:

+ CM makes obsolete a dual receiver approach for UTRA-FDD
± only so far foreseen means by 3GPP to allow for making measurements
- changing specified FDD parameters is rather complex
- fast power control is interrupted due to CM gaps
- parts of interleaving gain get lost
- only applicable if not already working with maximum power and lowest spreading factor
  (UE: $T_{\text{x max}} = 125 \text{ mW} \approx 20.97 \text{ dBm}, SF_{\text{min}} = 4$)
- mobile transmitters often need over-dimensioning
- additional interference arises

Regardless of specific disadvantages due to CM, there are other drawbacks with scanning other systems:
- additional power consumption for measurements
- signaling of measurement reports (for network controlled handover)
- continuous standby not possible
- absence announcement necessary (when in idle mode)

It was mentioned earlier that simulations in this chapter aim at illustrating the harmful impact of CM application on the system performance rather than providing detailed quantitative analyses. Therefore, certain simplifications were assumed concerning the scenario setup, mobility aspects and shadowing. However, further studies as in [136] confirm the negative effects of CM appliance. For the assumption that a 7-slot gap is used and every second frame is compressed with 20 ms interleaving, a direct impact on the uplink coverage area for real time service is calculated by a reduction of 2.4 dB. In a second example, a capacity degradation of 1.9 % is predicted if every third frame is compressed and 10 % of the users are simultaneously using the compressed mode. Worst-case assumptions with all users in CM simultaneously result in an average increase of the interference level of 19 % [136].

As a summary, one can say that compressed mode entails several drawbacks with respect to scanning complementary (vertical) systems. It was shown that CM application has a bad impact on both, the own performance (MT point of view) as well as the overall performance (System point of view). Accordingly, its application is not a preferable means of gathering necessary information on other systems as needed for handover control. A solution to this problem that avoids CM disadvantages has been introduced with the Hybrid Information System in Section 5. The potential gain of capacity/coverage in UMTS due to in-
formation gathering via the Hybrid Information System is indicated in Figure 8.5 by the shaded area.

8.3 Enhanced Coverage Detection

8.3.1 Coverage Detection

For optimized handover control, it is rather preferable to derive as good estimations on cell borders as possible. Obviously, (short-term) fading effects circumvent stable coverage borders. Mathematically, these effects can be modeled stochastically by introducing coverage probabilities for border areas. However, in order to derive a general statement on coverage borders, influences due to e.g., shadowing are first order impacts. Effects due to short-term fading are of superimposing nature for which they are not explicitly addressed in the following. Consideration is implicitly assumed due to averaging and smoothing. Presuming this, the coverage of an AP/BS depends on the following factors:

- Transmission Power
- Antenna gains of transmitting and receiving party
- Pathloss
- Receiver sensitivity

System specific impacts deriving from modulation, coding or spreading as well as minimum signal-to-noise ratios have implicitly been considered and are not further itemized. Accordingly, the area theoretically covered by one single AP/BS faces a deterministic extension and is sharply bounded. The borderline case results in a binary reception model indicating coverage (Rx status = 1) or no coverage (Rx Status = 0) as shown in Figure 8.6. The threshold is given by the minimum reception sensitivity $R_x$.

Figure 8.6: Binary reception model with reference coverage boundary
Hence, unlike as e.g. in [137] where the aim is to extend the coverage area, the aim here is to meet with the (theoretical) coverage boundary as precisely as possible. The scenario addressed is that the terminal is connected to a low bit rate RAT and needs to vertically handover to a high bit rate RAT as soon as possible. It was already shown in Section 8.2.2 that scanning is not a preferable means of detecting complementary system deployments. Hence, the Hybrid Information System shall be applied to provide the desired information. In order to trigger the availability of another system, HIS relies on previously gathered measurements supplying location related link state entries. Respective HIS databases as presented in Section 5.4 administer corresponding entries. Considering this information, a terminal’s current position is sufficient to determine whether a VHO would be successful or not. However, the coverage area derived from foreign party measurements does not comprise an accurate border as assumed in Figure 8.6, but can be better described as a transient and fuzzy area. Since fading was neglected, imprecise positioning is the main element of uncertainty. This is why HIS based VHO triggering needs to apply coverage detection algorithms on internally administered measurement data. The aim is to derive a sharp coverage boundary to be used in the decision process of VHO triggering.

### 8.3.1.1 Coverage Detection

The following section introduces a new algorithm that allows for accurate coverage boundary detection in spite of being dependent on measurements with inaccurate position information. Measurements being exploited are RPI histograms. For a detailed description of RPI histograms, please refer to Section 2.2.5.3.

Figure 8.7 illustrates reported RPI levels as a function of distance \( d \) from the transmitting party assuming free space propagation. An AP thereby has been placed at position \( d = 0 \) m, while a distant receiving station recognizes a corresponding RPI level \( R_{P_{rx}} \leq 7 \). With the propagation model according to equation (8.8) [157], the received signal power \( P_{rx} \) calculates as follows:

\[
P_{rx}(d) = \begin{cases} 
    P_s \cdot g_s \cdot g_r \left( \frac{\lambda}{4\pi d_0} \right)^2 & d \leq d_0 \\
    P_s \cdot g_s \cdot g_r \left( \frac{\lambda}{4\pi d_0} \right)^2 \left( \frac{d_0}{d} \right) \gamma & d > d_0
\end{cases}
\]

for \( d_0 = 1 \) m

\[(8.8)\]
$P_s$ is the transmit power which was chosen to 100 mW. No antenna gain was assumed so that $g_s$ and $g_r$ have been chosen to 1. $\lambda$ is the wavelength and $d$ is the distance between sender and receiver. The reference distance $d_0$ is chosen to 1m.

**Table 8.4: RPI histogram thresholds according to 802.11h [74]**

<table>
<thead>
<tr>
<th>RPI Level</th>
<th>Power Observed at Antenna (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$[-\infty, -87]$</td>
</tr>
<tr>
<td>1</td>
<td>$[-87, -82]$</td>
</tr>
<tr>
<td>2</td>
<td>$[-82, -77]$</td>
</tr>
<tr>
<td>3</td>
<td>$[-77, -72]$</td>
</tr>
<tr>
<td>4</td>
<td>$[-72, -67]$</td>
</tr>
<tr>
<td>5</td>
<td>$[-67, -62]$</td>
</tr>
<tr>
<td>6</td>
<td>$[-62, -57]$</td>
</tr>
<tr>
<td>7</td>
<td>$[-57, +\infty]$</td>
</tr>
</tbody>
</table>

**Table 8.5: Reference Sensitivity [69]**

<table>
<thead>
<tr>
<th>Modulation</th>
<th>Coding Rate R</th>
<th>Minimum Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPSK</td>
<td>1/2</td>
<td>-82 dBm</td>
</tr>
<tr>
<td>BPSK</td>
<td>3/4</td>
<td>-81 dBm</td>
</tr>
<tr>
<td>QPSK</td>
<td>1/2</td>
<td>-79 dBm</td>
</tr>
<tr>
<td>QPSK</td>
<td>3/4</td>
<td>-77 dBm</td>
</tr>
<tr>
<td>16QAM</td>
<td>1/2</td>
<td>-74 dBm</td>
</tr>
<tr>
<td>16QAM</td>
<td>3/4</td>
<td>-70 dBm</td>
</tr>
<tr>
<td>64QAM</td>
<td>2/3</td>
<td>-66 dBm</td>
</tr>
<tr>
<td>64QAM</td>
<td>3/4</td>
<td>-65 dBm</td>
</tr>
</tbody>
</table>

Figure 8.7: RPI levels and reference sensitivities for PHY-Modes
Realistic values for $\gamma$ are between 2 for free-space propagation and 5 for strong attenuation. Here, a value of 2.4 is chosen. According to Table 8.5, each combination of modulation and coding scheme (PHY-Mode) requires a minimum $R_x$ level (sensitivity) to come into operation. The according thresholds are indicated Figure 8.7 as well.

The resulting boundaries are best-case boundaries. Interference significantly decreases distances, which may be supported by a given PHY-Mode. As can be seen from Figure 8.7, MRs indicating RPI levels below RPI2 are not suited for any WLAN transmission due to minimum required BPSK1/2 sensitivity. The given sensitivity requirements hence result in a sharp theoretical maximum coverage distance.

### 8.3.1.1.1 Problem Description

An algorithm for VHO trigger generation must be able to identify the cell boundaries of a destination system. Imprecise localization introduces measurements that pretend coverage at positions actually not within the cell coverage area. These measurements are shown in Figure 8.8, displayed as white dots outside the cell. Obviously, these measurements in fact have been recorded inside the coverage area of the AP. Otherwise it would not have been possible for the reporting mobile to detect and report any signal at all. However, due to imprecise localization, the corresponding location that comes along with these reports was erroneously determined to be outside the covered AP area. A new terminal approaching the coverage area of the corresponding AP will request whether MR for its current position are available. If so, the corresponding MRs will be taken as basis for VHO decision. Recommending a VHO based solely on these reports would result in a handover try after whose execution the terminal would not be able to attach to the sought cell. For this reason, the white dots are referred to as ‘misleading’ reports.

On the other hand, one can rely on the fact that measurement reports indicated to be within the cell boundary are always ‘correct’; see black dots in Figure 8.8. Thereby, ‘correct’ does not mean that localization may not entail the same fuzzi-

---

35 In this investigation, one needs to distinguish between positioning of terminals that provide MR input to the HIS database (‘feeding clients’) and positioning of terminals that make use of HIS data (‘information clients’). Depending on given requirements, different accuracies may apply.
ness as for the misleading white dots. In fact, exactly the same fuzziness applies for these dots with the difference, that the position space representing the fuzzy sojourning area is completely covered by the AP.

Summarizing this, one needs to keep in mind that all reports categorized as ‘correct’ reports definitely were recorded inside the cell. Some reports categorized as ‘misleading’ reports obviously were recorded inside the cell, too, however, due to fuzzy positioning their location is assigned outside the actual coverage area. Finally, there is no report that could have been taken outside the coverage area but pretends to represent a covered position.

The problem for a possible handover algorithm now is to distinguish between misleading and correct reports. Since the sole existence of a measurement report obviously is no warranty that the target area is really part of the coverage area, some more sophisticated evaluation is to be applied. The proposed Centre of Gravity (CoG) algorithm, published by the author as related work in [68], exploits the fact that the density of misleading and correct measurement reports is of different nature.

![Diagram of Centre of Gravity Algorithm](image)

**Figure 8.8: Centre of Gravity Algorithm**

8.3.1.1.2 Centre of Gravity Algorithm

In order to derive a clear decision indicating whether coverage is given or not, a respective algorithm firstly needs to restrict to a limited number of measurement reports. Therefore, only local reports close to the cell border area should be considered. This is why a so-called Decision Area (DA), see Figure 8.8, was intro-
8.3. Enhanced Coverage Detection

The decision area defines an adjustable area around the MT’s position. A decision unit only considers entries within the DA to conclude whether a handover trigger is fired or not. Moreover, the introduction of the decision area allows fast database queries avoiding the necessity to search throughout a whole data set.

To support the decision algorithm, the Centre of Gravity (CoG) of all measurement reports within the decision area is calculated. The distance $d_{CoG}$ of the mobile terminal's position to the CoG is then compared to a threshold $Thd_{VHO}$ to generate the vertical handover trigger. With a well-populated long-term database, most of the measurement reports will be within the actual coverage area of the cell. Hence, a high MR density is given inside the actually covered area, while a low MR density outside the actually covered area adjusts, see Figure 8.8. Approaching the coverage area of a cell, the distance between a MT’s position and the calculated CoG follows a characteristic curve (see Figure 8.8). Assuming the localization error distribution to be zero-mean in the cell, the final distance between the centre of gravity and the mobile terminal's position will approach zero as soon as the entire DA is mapping the actually covered cell area.

Figure 8.8 exemplarily depicts the distance $d_{CoG}$ for a terminal approaching a cell. The distance firstly reported is the radius $R_{DA}$ of the decision area and measurement reports taken into account initially will be ‘misleading’ reports, see (1) in Figure 8.8. On further approaching the cell border, the distance $d_{CoG}$ will decrease until a local minimum (2) is reached. Since there are much more ‘correct’ measurement reports inside the actual cell than there are ‘misleading’ ones outside the cell border, the resulting distance $d_{CoG}$ will increase (3) again on further entering the cell. When the terminal itself approaches the actual cell border, the distance will adjust to $R_{DA}/2$. Once the mobile has moved into the cell, far enough so that the whole DA is within the coverage area, the distance $d_{CoG}$ will approach zero (4). By defining a minimal distance $d_{min}$, which needs to be below the local minimum introduced by the misleading measurements in (2), a handover decision can be generated. The corresponding minimal distance $d_{min}$ is also referred to as VHO trigger threshold $Thd_{VHO}$.

It should be noted that the algorithm's output actually is a distance vector. This vector $\vec{d}$ points from the mobile terminal's position towards the centre of the gravity of all measurement reports within the DA. In general, the distance vector $\vec{d}$ has the tendency to point into the direction of highest MR area penetration.
The angle between the velocity vector $\vec{v}$ and the distance vector $\vec{d}$ may be used to adjust the decision boundary $d_{\text{min}}$. Mobile terminals moving perpendicularly towards the cell border may have a higher $d_{\text{min}}$ compared to tangentially moving mobiles. This is how ping-pong vertical handovers for bypassing terminals due to false handover triggers can be minimized. Investigations for the given scenario have shown that $d_{\text{min}}$ should be chosen just about half of the decision area's radius for perpendicular movement.

### 8.3.1.2 Simulation Scenario

In order to visualize the 802.11h RPI Level histograms gathered from mobile terminals during communication, the following simulation scenario was used. Figure 8.9 depicts a small Manhattan scenario with one AP located at the scenario centre. Four buildings have been placed around the access point, each with a side length of 50 m. The interspace distance between buildings was chosen to 25 m.

![Simulation Scenario Diagram](image)

**Figure 8.9: Coverage detection scenario and results for exact positioning**

Within the scenario, MTs have been placed at random positions to take measurements in terms of Received Power Indicator (RPI) histograms according to 802.11h. Within extensive long-term simulation runs, more than 500 000 measurements are taken at a time resolution of 200 ms. Respective RPI histograms subsequently are derived, the corresponding position is determined and both pieces of information are provided to HIS for subsequent processing, see Figure 8.9. All simulation parameters have been summarized in Table 8.6.
Table 8.6: Scenario Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of Buildings</td>
<td>50x50 m</td>
</tr>
<tr>
<td>Street Size</td>
<td>25 m</td>
</tr>
<tr>
<td>Attenuation exponent $\gamma$</td>
<td>2.4</td>
</tr>
<tr>
<td>Wall attenuation</td>
<td>11.8 dB</td>
</tr>
<tr>
<td>802.11 Error Model</td>
<td>C/I Table based Random Error</td>
</tr>
<tr>
<td>Mobile Velocity</td>
<td>20 km/h</td>
</tr>
<tr>
<td>MR Interval</td>
<td>200 ms</td>
</tr>
<tr>
<td>Measurement Duration</td>
<td>10 ms</td>
</tr>
</tbody>
</table>

8.3.1.2.1 Link State- and Coverage Map

Based on the given input data, HIS (long-term) databases have been used to visualize the RPI measurements resulting in so-called link state- or coverage maps. For each position in the map, all measurement reports are evaluated by calculating the reported mean RPI Level. This value is represented by an associated color. Positions, for which no measurements are available, have been assigned RPI Level 0. The access point is located at $x = 500$ m and $y = 500$ m. It can be seen that the maximum range that may be covered by the access point is about 191 m away from the cell centre. Communication is not possible when the received power drops below -82 dBm, which is the minimal sensitivity level required for BPSK1/2, cp. Table 8.5. The map does not show any measurements with RPI 1. This is because no communication can be supported at that RPI Level (compare Figure 8.7, Table 8.5). Further, communication with the AP is not possible behind buildings. The wall attenuation is too strong so that the received power is below the minimal threshold of -82 dBm. However, received power within buildings is still high enough to enable communication. RPI values found within buildings are between RPI3 and RPI4.

The visualization presented in Figure 8.9 is based on RPI measurements with exact positioning to be used as reference link state map and validation of the correct behavior of the simulation environment. In reality, however, exact position information is not available.

The right part of Figure 8.10 shows simulation results considering erroneous positioning.
Such, real link state maps will reflect a picture more similar to Figure 8.10 b) rather than Figure 8.10 a). Erroneous positions are modeled by drawing a location error being added to the exact position. A detailed description of location error modeling has been provided in Section 6.1. For this scenario, a Gaussian error distribution with zero mean and variance of $\sigma_x^2 = \sigma_y^2 = 100 \text{ m}^2$ was used, whereby the maximal error distance was limited by the cut-off distance $r_{\text{cut}} = 10 \text{ m}$.

It can be seen from Figure 8.10 b) that imprecise positioning results in fuzzy RPI zones with smooth transitions between received power indicators. Some measurement reports indicate incorrect values compared to the results shown in Figure 8.10 a). Within the buildings there are RPI Levels reported that belong to the area outside the buildings, some measurements imply that there is coverage behind buildings, too. Having a look at the upper right quadrant of the scenario one can also see that the density of (misleading) measurement reports outside cell borders (1) is lower than within the cell. Furthermore, there is no longer a sharp borderline between RPI zones (2).
The effect of fuzzification is a direct consequence of the localization error. Distributions that have higher probabilities for high errors than for small errors will inherently feature by increasing fuzzy cell borders and fuzzy RPI transition zones. The next chapter shows how this property is exploited by the proposed cell border detection algorithm.

8.3.1.3 Cell Border Detection Algorithm: Centre of Gravity

The following section evaluates the proposed Centre of Gravity algorithm for cell border detection. For this, the same long-term data that was used to generate the link state maps from Figure 8.10 b) (fuzzy positions) is used as input data. To decide whether a mobile is within the coverage area of the 802.11 cell, a decision area is drawn around the mobile terminal’s position. The radius of this area was set to \( R_{DA} = 5 \) m. Hereafter, the CoG algorithm is applied with different thresholds \( d_{\text{min}} \) respectively. Figure 8.11 shows the distance \( d_{\text{CoG}} \) from a fictitious mobile position to the CoG of all measurement reports within the decision area. This resembles the link state maps shown in the previous section. Outside the cell coverage, there are no HIS measurement entries at all. At those positions, \( d_{\text{CoG}} \) was defined to be 5 m, corresponding to the maximum radius of the decision area \( R_{DA} \).

![Figure 8.11: Distance \( d_{\text{CoG}} \) to CoG](image1)

![Figure 8.12: Distance \( d_{\text{CoG}} \) to CoG cut along x-Axis, \( y = 500 \) m](image2)
Figure 8.13: Characteristic curve for CoG cell border detection

Figure 8.12 shows a cut of the distance map of Figure 8.11 along the x-Axis through the access point at y = 500 m. It can be seen that the distance $d_{CoG}$ significantly decreases after entering the cell. Being of particular interest, a close-up of the cell border area corresponding to $300 \leq x \leq 320$, $y = 0$ is depicted in Figure 8.13. It can be seen that the theoretically derived characteristic curve with its 4 phases as described for the CoG algorithm in Section 8.3.1.1 is recognized for analysis as well as for simulation results: Mobile terminals approaching the cell border initially observe a decrease of the distance to the centre of gravity due to ‘misleading’ measurement reports outside the cell's coverage area (1). On further entering the cell, $d_{CoG}$ increases again due MR density rise, resulting in the characteristic local minimum (2). Further approaching the cell border, $d_{CoG}$ slightly increases again (3). Once the DA completely maps with the covered cell area, $d_{CoG}$ adjusts to an absolute minimum (4). Figure 8.13 provides a comparative view on the four phases for both, simulation results and analysis.
Once the characteristic CoG curve is derived, a reasonable threshold $\text{Thd}_{V\text{HO}}$ needs to be appointed. Figure 8.13 shows white areas where coverage was detected and black areas where no coverage was detected. First, $\text{Thd}_{V\text{HO}}$ was set to 1.5 m, which is above the local minimum introduced by misleading reports. It can be seen that coverage is ‘detected’ at positions outside the cell’s actual coverage area, e.g., there are some white areas behind buildings. Better results are achieved for a reduced threshold of $\text{Thd}_{V\text{HO}} = 0.9$ m. However, if the decision threshold is chosen too small, e.g., $\text{Thd}_{V\text{HO}} = 0.2$ m, other drawbacks come into operation. It is to mention that no further misleading detection outside the covered area is reported, but obviously at the cost of non-reliable detection inside the actually covered area.

The introduction of black areas inside the actually covered cell indicates that no coverage was detected though signal strength would be sufficient. In addition, it is to say that lowering of $\text{Thd}_{V\text{HO}}$ results in delayed coverage detection for the approaching terminal.

An acceptable compromise to ensure correct detection hence is the threshold $\text{Thd}_{V\text{HO}} = 0.9$ m, which allows safe detection while the introduced ‘delayed’ detection of about 2.5 m (values depend on terminal velocity) to the actual cell border is minimized though, see Figure 8.13.

Obviously, optimum $\text{Thd}_{V\text{HO}}$ adjustment is scenario and service dependent. In contrast to the characteristic curve that is based on long-term measurements and thus is of static nature, the adjustable parameter $\text{Thd}_{V\text{HO}}$ represents one degree of freedom in the coverage detection process. Depending on the aspired accuracy and reliability of the cell coverage detection, this parameter needs to be adjusted while an upper limit $\text{Thd}_{V\text{HO}}$ according to the local minimum introduced by the centre of gravity algorithm needs to be kept. Performance figures with respect to $\text{Thd}_{V\text{HO}}$ adjustment and others are presented in the following.

### 8.3.2 CoG Trigger Performance

So far, coverage detection concentrated on evaluation of erroneous position information within the HIS database, while the position of the requesting party was assumed to be sufficiently well known (compare footnote 35 on page 203 on ‘feeding clients’ and ‘information clients’). The following Section considers erroneous positioning of both, feeding clients as well as information clients.
In addition, two other harmful impacts are separately considered to provide an encompassing view on the coverage-detection and trigger-generation problem within heterogeneous system environments.

Appropriate trigger generation of the CoG algorithm depends on three parameters:

- Decision Threshold $T_{d_{CoG}}$ (see Figure 8.13)
- Number of measurements within the database
- Positioning error

The CoG algorithm performance using erroneous localization is evaluated in the scenario shown in Figure 8.14. A MT whose starting point is chosen randomly approaches the coverage area of a WLAN access point at a constant velocity of $v = 5$ km/h. The terminal initially is connected via UMTS that supports continuous localization in time steps of 200 ms. HIS takes the terminal’s location as input, applies CoG coverage detection against its internal database entries and fires a VHO trigger as soon as appropriate. The radius of the CoG decision area (not shown in the figure) was chosen to 5 m. Evaluation metric is the distance $d$ of the mobile terminal to the reference cell border as introduced earlier, cp. Figure 8.6 and Figure 8.7, at the time when the VHO is triggered.

![Figure 8.14: CoG Simulation Scenario](image-url)
Top 1) Figure 8.15 shows the impact of different threshold values $\text{Thd}_{\text{CoG}}$ on the trigger distance distribution. It can be seen that with increasing threshold more and more handovers are triggered too early, i.e., the trigger is fired though the terminal has not yet reached the actual coverage boundary. This result is in-line with the results presented in Figure 8.13. Applying an over-dimensioned threshold shifts the operating point of the CoG to the characteristic local minimum area (2). Stations that rely on this VHO recommendation will not be able to associate with the new system and need to fall back to the old one, where they will be provided another VHO trigger. Over-dimensioning of CoG threshold $\text{Thd}_{\text{CoG}}$ hence results in undesirable ping-pong handovers.

![Distribution of VHO Triggers](image)

**Figure 8.15: Distribution of VHO trigger distances for different CoG thresholds**

Top 2) Figure 8.16 shows the impact of different measurement densities on the accuracy of the handover decision. Evaluation metric is again the distance $d$ of the mobile terminal to the theoretical reference cell border when VHO is triggered. The CoG algorithm threshold this time was set to a fixed value of $\text{Thd}_{\text{VHO}} = 0.25$ m. Database entries based on third party measurements are assumed to be erroneous Gaussian with a variance of $\sigma_x^2 = \sigma_y^2 = 100$ m$^2$ and a maximum error of $r_{\text{cut}} = 10$ m. Positioning of the moving terminal itself is assumed to be error-free.
Figure 8.16 points up the performance of trigger generation for different numbers of measurements in the database. The parameter $n = 10$, 25, 50 and 100 measurements indicates the number of database entries based on which the CoG algorithm was applied (this corresponds to the number of entries covered by the 5 m radius decision area, cp. Figure 8.8). It is shown that trigger generation performs the better, the higher the density of measurement entries in the database. For e.g., $n = 100$, all handover have taken place after approximately $d = 35$ m. For $n = 50$ however, it takes approximately $d = 78$ m until all handover have been proceeded.

A drawback is that with increasing number of database entries, an enhanced probability for occurrence of ‘misleading’ (cp. Figure 8.8) measurement reports is given. This is why for $n = 100$ up to 20 % of the handover decisions are made too early.

Top 3) Figure 8.17 finally concentrates on the harmful impact of localization errors of the terminal (information client). Different values for standard deviation and cut-off criterion according to the legend in Figure 8.17 apply. The rightmost curve represents the handover distance distribution for error-free localization of the mobile terminal. Performance of CoG trigger generation decreases with increasing positioning error resulting in more and more handovers being
triggered before the actual cell border has been reached. The harmful results are ping-pong handover as described for Top 1).

![Distribution of VHO Triggers](image)

**Figure 8.17: CDF of VHO triggers distance for different localization errors**

Very late handover decisions beyond trigger distances of $d = 15m$ do no longer depend on the maximum localization error. Since the decision area has completely entered the actually covered area (cp. case 4 in Figure 8.8), trigger generation is only subject to the chosen threshold $\text{Thd}_{\text{CoG}} = 0.25$ and the measurement distribution/density (investigated in Top 2), both of which being the same for all five curves.

Within this Section 8.3, the overall problem of coverage detection of other systems has been addressed. In order to optimize handover control, it is preferable to derive estimations on cell borders as precisely as possible. Natural fluctuations due to e.g. short-term fading are of superimposing nature and have not been explicitly addressed. In order to derive an objective measure, a reference cell border being based on receiver sensitivity requirements was defined. Performing coverage detection is highly dependent on localization errors. A classification of reliable and non-reliable MR joint with position information was given in terms of ‘misleading’ and ‘correct’ MR. With the introduction of the Center of Gravity (CoG) algorithm, a new method was introduced that ensures best-suited coverage detection even in case of erroneous localization. Important
parameters for the CoG are the size of the decision area and the decision threshold that needs to be chosen below a characteristic local minimum in the evaluation curve. Both parameters require professional expertise to be chosen correctly, e.g. over-dimensioning of the CoG threshold results in ping-pong handover. However, being related to the local geo-environment, non-professionals could work with the CoG once the thresholds have been determined. Further dependencies of the reliability of coverage detection and VHO triggering consider MR density in related databases and impact of the localization error. For the latter it is obvious, that coverage detection performs best for negligible localization errors (standard deviation < 5 m, cut-off criterion < 12 m). Considering MR densities, CoG performs the better, the more MR in HIS databases are available.

8.4 Context Provisioning

The previous section has worked out that measurements in conjunction with location data are exquisitely useful. Corresponding link state maps form the basis of all other actions, be it general heterogeneous system detection or improved VHO control.

While the focus was put on when trigger generation should take place, the following section discovers what data can be provided in addition to the sole handover directive. Initially, the focus is put on optimization of capacity in terms of throughput from a single user’s perspective (Section 8.4.1) and hereafter throughput optimization for an entire Hot Spot is aspired.

8.4.1 Recommendation of initial PHY-Mode

Measurement reports gathered by feeding clients may be used to support link adaptation for handover candidate information clients. In addition to sole VHO trigger generation, the Hybrid Information System may provide additional information to the handover candidate, such as expected link quality. Benefits are twofold: First, the station can decide whether an aspired service probably will be supported (e.g., high bandwidth requirements) and second, selection of initial PHY-Mode is possible right from the beginning.
The following section investigates possible benefits due to appropriate initial PHY-Mode selection. The link adaptation algorithm implemented within the S-WARP protocol simulator has been modified to consider initial PHY-Mode recommendation from HIS.

### 8.4.1.1 Link Adaptation Algorithm

The impact of initial PHY-Mode recommendation by HIS on system performance was evaluated by using a windowed Link Adaptation (LA) algorithm\(^ {36} \). The initial algorithm being based on [70] has been modified and enhanced to model different LA behaviors.

The 802.11 MLME monitors the link state by keeping a history of received ACKs and NACKs. Whenever ACK or NACK is received, this information is stored to respective ring buffers. Three different window sizes according to short, mid- and long-term changes of the link state have been implemented. Initial entries in the long window hereby resemble entries in the medium window that in turn resembles entries from the short window. Figure 8.18 depicts possible buffer states. Arriving ACK or NACK messages are queued foremost of all three ring buffers.

![Figure 8.18: Windowed Link Adaptation Algorithm (based on [70])](image)

\(^{36}\) Link Adaptation is not subject to the specification. Manufacturers are free to implement proprietary algorithms. The windowed algorithms applied in this thesis allows for emulation of different possible LA properties.
Every time the ring buffers are updated, a decision is made on switching to a higher PHY-Mode, on switching to a lower PHY-Mode or on keeping the current one. The decision is found by calculating the ratio of NACKs within all windows according to

$$R_{s,m,l} = \frac{N_{\text{NACK}s,m,l}}{W_{s,m,l}}$$  \hspace{1cm} (8-1)

Thereby, $R_{s,m,l}$ denotes the ratio of NACKs within the respective window and $N_{\text{NACK}s,m,l}$ the number of NACKs found within that window. The window size $W_{s,m,l}$ is 5, 15 or 25. Only if all windows are filled the decision to switch to a higher PHY-Mode is made by calculating a compound ratio $R$ using:

$$R = \sum_{i=s,m,l} w_i R_i, \quad \text{with} \quad w_s = \frac{5}{10}; \quad w_m = \frac{3}{10}; \quad w_l = \frac{2}{10}$$  \hspace{1cm} (8-2)

The weighting factor $w$ is applied to add different weights to the respective ring buffers. Based on empiric results, upper and lower limits for $R$ have been derived. A ratio below $R_{\text{up}} = 0.044$ indicates good link quality for which a higher PHY-Mode will be chosen. Ratios above $R_{\text{down}} = 0.45$ result in application of lower PHY-Modes. No changes are applied for any intermediate value.

If windows are not completely filled, only the short and medium windows are taken into account but different thresholds apply: If $R_s > 0.6$ or $R_m > 0.4$, the PHY-Mode is switched down, otherwise, there are no changes. This mechanism shall prevent non-appropriate long transmissions at high PHY-Modes in the initial phase of communication.

Figure 8.18 gives an exemplary snapshot of the three ring buffers. Since all windows have been filled, both switching directions, up and down, are possible. The resulting ratios $R_{s,m,l}$ calculate to

$$R_s = \frac{1}{5}; \quad R_m = \frac{4}{15}; \quad R_l = \frac{6}{25},$$  \hspace{1cm} (8-3)

for which the weighted ratio $R$ according to equation (8.2) results to

$$R = \frac{5 * 1}{10} + \frac{3 * 4}{15} + \frac{2 * 6}{25} = \frac{57}{250} = 0.228,$$  \hspace{1cm} (8-4)

which means that the LA in this example does not trigger any switching action.

To investigate the impact of PHY-Mode recommendation on fast and slow Link
Adaptation algorithms the window sizes used by this implementation were parameterized by multiplication with a factor $f$. Preliminary simulations have been carried out to determine the LA dynamicity. The evaluated scenario consists of one mobile and one AP being settled close to each other with optimum link quality. Since dynamicity of the LA depends on the arrival rate of $ACK$s and $NACK$s, the offered load was chosen to exceed system capacity, even when using the 54 Mbit/s PHY-Mode. Applying an initial PHY-Mode of 6 Mbit/s, Figure 8.19 shows PHY-Mode adaptation over time for different window sizes $f$. It can be seen that the larger the window size is, the longer it takes to reach the 54 Mbit/s PHY-Mode.

![Dynamic Switching Behaviour of Link Adaptation Algorithm with different Window Sizes](image)

**Figure 8.19: Dynamicity of Link Adaptation**

One can state, that fast switching is appropriate in highly dynamic scenarios with instable or fast changing link conditions. Many switching actions however, entail the risk of unstable operation resulting in more signaling overhead, more re-transmissions, increased power consumption, and harmful impact on system control (e.g., power control algorithms). On the other hand, delayed adaptation of the PHY-Mode results in suboptimal exploitation of the radio resource. Fast and slow switching characteristic of LA in the following are referred to as *progressive* and *conservative* behavior. Emulation of one or the other is performed by applying different window sizes $f$. 
8.4.1.2 Scenario Description
For evaluation of initial PHY-Mode recommendation during VHO, the Manhattan scenario as introduced in Section 8.3.1 was used. Four buildings have been placed around one AP. One mobile terminal moves from behind the top left building into the coverage area of the AP. On entering WLAN, the Hybrid Information System triggers VHO handover to the terminal while at the same time proving an initial PHY-Mode recommendation.
Comparing the scenario with link state maps from HIS (see Figure 8.7) shows an RPI3 level at the position where the terminal enters the WLAN. With respect to reference sensitivity power levels defined for each PHY-Mode, it can be seen that QPSK ¾ (18 Mbit/s) is a suitable recommendation.

![Handover Scenario](image)

**Figure 8.20: Handover Scenario**

In the following, potential gains of the presented approach are presented. HIS triggered initial PHY-Mode recommendation is compared to ordinary schemes starting with BPSK ½ and applying progressive or conservative LA.

8.4.1.3 Evaluation of Throughput Gain
Figure 8.22 shows resulting throughput for vertical handovers of mobile terminals using the described link adaptation algorithm. Different window sizes of \( f = 1, 2, 3 \) are applied. The x-Axis shows the time that has passed since vertical handover occurred. The leftmost curve represents throughput performance of mobile terminals entering the 802.11 cell with initial PHY-Mode recommendation by HIS.
The point of vertical handover is chosen so that the mobile terminal enters the cell at the reference cell border. It can be seen that maximum throughput is reached first by stations that rely on initial PHY-Mode recommendation by the Hybrid Information System. All other stations reach the maximum throughput later according to dynamicity as explained by Figure 8.19. The larger the window size being used by the LA algorithm, the slower is the throughput increase. Finally, all stations end up in using 16 QAM \( \frac{1}{2} \) (24 Mbit/s) that is the highest PHY-Mode that is just about to be applied for RPI 3 (see Table 8.5 and Figure 8.7).

Table 8.7 shows the approximated additionally transferred volume when choosing an initial PHY-Mode of 18 Mbit/s for this scenario. This is visualized by the shadowed area in Figure 8.22. One can see that context provisioning allows for increased transfer volumes of more than 1 MB compared with conventional schemes.
Table 8.7: Gain due to initial PHY-Mode recommendation

<table>
<thead>
<tr>
<th>Longest Window Size of Link Adaptation</th>
<th>Additional Transfer Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 (f=1)</td>
<td>450 kbit</td>
</tr>
<tr>
<td>50 (f=2)</td>
<td>880 kbit</td>
</tr>
<tr>
<td>75 (f=3)</td>
<td>1250 kbit</td>
</tr>
</tbody>
</table>

It is to say that the magnitude of the above given values needs to be seen as an example, simply to demonstrate that further improvements due to HIS are possible. The actual task of HIS is to relieve stations of the necessity for self-conducted scanning, coverage detection, and QoS based trigger generation. Recommendation of initial PHY-Mode is just a nice add-on, but it can be provided at no additional cost and it pays off. Possible gains are scenario specific and dependent on shadowing, maximum saturation throughput (packet size), user velocity, implementation of LA, and others.

While this section concentrated on optimization of one single user’s throughput, the following section puts the focus on optimization of capacity of the entire Hot Spot. Channel occupation is an important key word herein: Performing VHO and applying suboptimal (low) PHY-Modes unnecessarily wastes capacity. Hence, it will be shown that sophisticated VHO control by HIS entails some further advantages being of great benefit not just for a single station but for all other residing stations in the Hot Spot.

8.4.2 Capacity Exploitation

It is widely known that efficiency of carrier sense based protocols such as legacy 802.11 decreases with application of more complex PHY-Modes (cp. e.g., [86]). Protocol inherent time durations, needed for scanning and control of medium access, prevent stations from transmitting user data. Nonetheless, in order to optimize a Hot Spot’s performance in terms of throughput, all transmissions ideally apply 64 QAM ¼. Obviously, this is only possible for good link conditions close to the AP. Due to decreasing signal power reception, more robust PHY-Modes need to be applied for increasing distances to the centre. Reference distances for which a particular PHY-Mode is just about to be used result from requirements on receiver sensitivities (to be further addressed in Section 8.3.1.1). According to the denotation ‘cell border’, the term ‘PHY-Mode border’ is applied henceforth to refer to respective reference distances, cp. Figure 8.23.
The CSMA/CA algorithm of legacy 802.11 targets on exclusive temporarily assignment of the medium to one single station. The outcome of this is that throughput maximization for the overall system can only be achieved for exclusive medium access by stations within the 54 Mbit/s PHY-Mode border. Figure 8.24 gives an exemplary illustration: At first, MT1 and MT2 compete for the medium. Both are settled within the 54 Mbit/s PHY-Mode border. The overall capacity being conveyed within a time span $\Delta T$ results in a virtual reference volume of 270 data units. Hereafter, MT 3 and MT 4 compete for the medium. Being settled at the cell border, transmissions of MT3 can only take place at 6 Mbit/s for which the medium is busy for a longer period, if the same data volume is to be transmitted. The reference value for the overall capacity being conveyed in the same time span $\Delta T$ now is reduced to 66 data units.
To investigate the impact of overall capacity reduction within WLAN due to VHO, the scenario depicted in Figure 8.23 was evaluated. Four mobile terminals have been placed within the centre of the Hot Spot, being supplied with 54 Mbit/s PHY-Mode. The offered load was increased until capacity limit was reached resulting in a saturation throughput of 16.1 Mbit/s.

A fifth station initially is connected to UMTS and approaches the coverage area of the AP. Within a first simulation run, the station is triggered to handover as soon as Hot Spot coverage is reached. Since link quality is rather poor at the cell border, initial PHY-Mode selection chooses BPSK ½. Within subsequent simulation runs, trigger generation for VHO is delayed until another PHY-Mode border was reached, cp Figure 8.23. According to Section 8.4.1, the VHO trigger is fired together with recommendation of the initial PHY-Mode to be applied for further transmissions. That way each PHY-Mode border was investigated by evaluating the overall system throughput.

Table 8.8 shows the services that mobile terminals use during this simulation along with resulting offered load. Each of the stations in the centre maintains a VoIP connection plus file transfer with high load requirements. The arriving mobile terminal is assumed to enter the cell maintaining an active VoIP connection, which has been started in UMTS. Additionally it initiates file transfer as soon as it enters the Hot Spot.

Table 8.8: Scenario Service Parameters

<table>
<thead>
<tr>
<th>Service</th>
<th>Uplink</th>
<th>Downlink</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centre Station (each)</td>
<td>192 kbit/s</td>
<td>5000 kbit/s</td>
<td>VoIP + file transfer</td>
</tr>
<tr>
<td>Moving Station</td>
<td>128 kbit/s</td>
<td>128 kbit/s</td>
<td>VoIP</td>
</tr>
<tr>
<td>(prior to VHO)</td>
<td>128 kbit/s</td>
<td>128 kbit/s</td>
<td>VoIP</td>
</tr>
<tr>
<td>Moving Station</td>
<td>64 kbit/s</td>
<td>1152 kbit/s</td>
<td>file transfer</td>
</tr>
<tr>
<td>(after VHO)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 8.25 shows the resulting downlink system throughput as a function of the entry PHY-Mode. In addition, the system throughput prior to VHO is illustrated for comparison. It can be seen that there is a significant degradation of the system throughput due to VHO, especially if being triggered at the cell border. While the initial saturation throughput generated by four stations was approx. 16 Mbit/s, it decreases to 12 Mbit/s for five stations. Hence, a station entering the
cell at PHY-Mode BPSK ½ reduces the resulting system throughput by approximately 4 Mbit/s. Considering only the throughput of the four primary stations, they even face a loss of 5.6 Mbit/s.

It is shown from Figure 8.25 that the harmful impact of VHO on the overall capacity declines with increasing PHY-Mode border used for triggering. This is inline with the illustration from Figure 8.24. Another conclusion to be drawn is that decrease of overall capacity for lower entry PHY-Mode really is given due to increased busy times of the channel and not due to increased number of collisions with subsequent backoffs. This is also confirmed for evaluation of the up-link as shown in Figure 8.26. The system is able to carry the additional offered load and system throughput is increased for this direction.

![Figure 8.25: System Throughput (DL)](image)

![Figure 8.26: System Throughput (UL)](image)

Results from this section have shown that VHO to WLAN may result in performance degradation not just for already associated stations within the Hot Spot but for the entire cell. Since transmissions at low PHY-Modes occupy the channel longer than at high PHY-Modes, scenarios working close to saturation suffer significantly from low PHY-Mode ‘disturbers’ and hence should be ‘protected’. A possible solution to this problem was presented in this section: Trigger generation for VHO should incorporate so called PHY-Mode borders. It is worth mentioning that application of this concept in fact results in virtually shrinked Hot Spot coverage but at the benefit of optimized system capacity in terms of throughput. For some cases, it might even be in the interest of the handover can-
didate, if VHO to WLAN is deferred until a specific PHY-Mode border is reached. For instance, if the reason for aspired VHO is initiation of a particular service with extraordinary high bandwidth demands\textsuperscript{37}, it is pointless to handover before a PHY-Mode border is reached at that the target cell (theoretically) is able to support respective data rates.

The realization of PHY-Mode border aware trigger generation can easily be supported by the Hybrid Information System. Disposing of link state maps, PHY-Mode borders are inherently known. In addition, information on the current load in the WLAN cell can further be taken into account. When triggering VHO, the initial PHY-Mode to be applied can directly be provided according to Section 8.4.1.

**8.5 Adaptive Beacon Control**

So far, a couple of use cases for location-based networking have been investigated. A further highlight will be presented in the following showing that information administered by the Hybrid Information System is rather useful to control and adapt transmission of system information. Successful handover to another system requires prior synchronization. The Hybrid Information System offers effective support in the sense that general existence, current availability, and supported services can be reported to a handover candidate terminal. In addition, parameters that allow for faster execution of the synchronization procedure can be provided as well.

The following section investigates the beacon’s influence on the overall system performance and presents proposals how the Hybrid Information System can be deployed to control optimum beacon broadcast in an integrated system environment. Related work has been published by the author in [130].

**8.5.1 Control of Beacon Interval**

In principle, WLAN 802.11 beacon intervals can comprise any time span between approximately 1ms and 1 minute with a granularity of time units (1024

\textsuperscript{37} Ongoing discussions with respect to killer applications for broadband DSL currently focus on VoD services. T-online and Arcor Germany already today offers respective premium services at 2 Mbit/s. It is likely that if successful for fixed access, similar services will be expanded to be offered wirelessly, too.
However, the specification does not prescribe any particular period. As long as there is no new terminal to associate with the network, transmission of beacon information introduces additional load to the system. Unnecessarily allocating resources, beacon transmission results in signaling overhead and may even decrease the overall throughput. A beneficial property hence would be to adapt the static beacon interval to current needs, resulting in *adaptive beacon intervals*. If no new station is expected to arrive, transmission of the beacon can be reduced or even omitted.

### 8.5.1.1 Throughput Optimization

The maximum possible throughput that can be achieved in WLAN 802.11 depends on a variety of parameters: Apart from link conditions, the protocol itself leads to different peak data rates as explained in the following: The CSMA/CA based 802.11 channel access with related protocol inherent backoff times introduces idle periods that may not be used for data transfer. Prevention of unnecessary signaling overhead directly results in increased throughput. Figure 8.27 depicts simulation results for achievable peak data rates of 802.11 for ideal link conditions and a fixed PHY-Mode of BPSK $\frac{1}{2}$. No hidden stations are assumed for which RTS/CTS signaling is disabled. The resulting saturation throughput $TP_{\text{sat}}$ depends on the chosen packet size $L_{\text{packet}}$.

$$TP_{\text{sat}} = \frac{P_e \cdot L_{\text{packet}}}{T_{\text{slot}}}$$

This is also expressed by equation (8.9) that allows an analytic estimation of the saturation throughput as a function of the probability $P_e$ for successful transmission and the mean transmission duration $T_{\text{slot}}$ [159].

Simulation results presented in Figure 8.27 are inline with previous investigations. A performance analysis calculating the saturation throughput of the legacy 802.11 DCF based on a Markov model has been presented by Bianchi in [158]. Enhancements to this model with respect to backoff delay have been introduced by Hettich in [159]. With the introduction of 802.11e for QoS support, access priorities have been specified for which a modified version of the model has been presented by Mangold in [86] to evaluate concepts of the *Enhanced Distributed Channel Access (EDCA)*\(^{38}\) contention window.

---

\(^{38}\) Previous draft version of 802.11e defined the *Enhanced Distributed Coordination Function (EDCF)* that was replaced by EDCA in the final specification.
However, none of the previously mentioned workings addresses the extraordinary importance of the beacon and its impact on synchronization and system throughput. Figure 8.27 shows that the packet size does not affect the resulting throughput for low and moderate system loads up to 2500 kbit/s. With further increasing offered load, the resulting saturation data rate depends on the chosen packet assembling. Throughput optimization for good link conditions at high load conditions is achieved with large packet sizes. This, however, affects control data delivery within legacy 802.11 because beacons might be delayed due to busy medium. Accordingly, target beacon transmission times cannot be guaranteed but become dependent on the current load in the system. To allow for deterministic reception of system information, 802.11e introduced beacon protection as explained in Chapter 2.2.2. Stations\(^{39}\) with a valid TXOP are only allowed to initiate a frame exchange, if being completed prior to the next TBTT, otherwise they need to defer and wait. Since TXOP is still with the deferring

\(^{39}\) Investigations in this thesis assume exclusive presence of QoS enabled stations according to 802.11e. Harmful impacts of legacy stations have been investigated in [86] and are out of scope of this work.
station, no other station is allowed to transmit for which a transmission gap results, see also Figure 6.11. Analytical results from Section 6.4 will be compared to simulation results in the following.

Figure 8.28 indicates the harmful influence of beacon protection on the overall system throughput. A fixed PHY-Mode of 6 Mbit/s is assumed. Similar to Figure 8.27, the offered load in the system is increased until saturation of the carried throughput is reached. This time, however, the packet size has a fixed value of $L_{\text{packet}} = 1024$ byte (large packet size for optimized TP; only one packet per frame exchange; no fragmentation) but the beacon interval is varied. As long as the system is not close to saturation, i.e., $\text{Load}_{\text{offer}} < 4500$ kbit/s, the beacon interval only has a minor impact on the resulting throughput. In between two TBTTs, there is enough time for data delivery. Working close to saturation, beacon protection results in inefficient idle transmission gaps. Since there is no opportunity to transmit buffered packets from deferred stations in the next frame, the resulting data rate decreases with increasing beacon frequency. The difference of peak data rates $TP_{\text{sat}}$ with beaconing at $\Delta \text{TBTT} = 10.24$ ms (= 10 TU) period and $\Delta \text{TBTT} = 1024$ ms (= 1000 TU) period amounts to 322 kbit/s (Figure 8.28). For increased packet sizes of $L_{\text{packet}} = 2048$ byte, the resulting difference is even 721 kbit/s (Figure 8.29).

The given results match well with analysis from Section 6.4 as shown in the following:
For a beacon size of 100 byte, the resulting Management MAC-PDU comprises 128 byte, including a 24-byte MAC frame header and a 4-byte CRC frame check sequence. Applying equation (6.17) and (6.18), the number of required OFDM Symbols $\sum N_{OFDM\_beacon}$ calculates to

$$\sum N_{OFDM\_beacon} = \frac{16 \text{ bit} + 8 \times (100 + 24 + 4) \text{ byte} + 6 \text{ bit} + 10 \text{ bit}}{N_{\text{SAMP} (BPSK/2)}} = 44 \text{ Symbols} \quad (8.10)$$

The beacon duration $T_{\text{beacon}}$ is given by multiplying $\sum N_{OFDM}$ with the OFDM symbol duration and adding further durations for physical synchronization and control data according to equations (6.15) and (6.16):

$$T_{\text{beacon}} = \frac{T_{\text{preamble}} + T_{\text{Signal}} + 44 \text{ Symbols} \times 4 \mu s / \text{Symbol}}{\sum N_{OFDM} \times T_{\text{Symbol}}} = 196 \mu s \quad (8.11)$$

In a similar manner, the frame transmission durations $T_{\text{frame\_1024}}$, $T_{\text{frame\_2048}}$ of MAC PDUs of length $L_{\text{packet}} = 1024$ byte and $L_{\text{packet}} = 2048$ byte are computed. Applying equation (6.17) gives the number of required OFDM symbols,

$$\sum N_{OFDM\_1024} = \frac{16 \text{ bit} + 8 \times (1024 + 24 + 4) \text{ byte} + 6 \text{ bit} + 10 \text{ bit}}{N_{\text{SAMP} (BPSK/2)}} = 352 \text{ Symbols} \quad (8.12)$$

and

$$\sum N_{OFDM\_2048} = \frac{16 \text{ bit} + 8 \times (2048 + 24 + 4) \text{ byte} + 6 \text{ bit} + 2 \text{ bit}}{N_{\text{SAMP} (BPSK/2)}} = 693 \text{ Symbols} \quad (8.13)$$

so that
8.5. Adaptive Beacon Control

\[ T_{\text{frame}_{\text{1024}}} = 16 \mu s + 4 \mu s + 352 \text{Symbols} \times 4 \mu s / \text{Symbol} = 1428 \mu s \]
\[ T_{\text{frame}_{\text{2048}}} = 16 \mu s + 4 \mu s + 693 \text{Symbols} \times 4 \mu s / \text{Symbol} = 2792 \mu s. \]

The backoff duration \( T_{\text{backoff}} \) is derived under the assumption that no collisions have appeared for which the contention window has a minimum size of \( CW_{\text{min}} = 15 \), cp. Section 2.2.1. Being equally distributed between \([0, CW_{\text{min}}]\), a mean value of \( CW_{\text{mean}} = 7.5 \) is considered resulting in

\[ T_{\text{backoff}} = CW_{\text{mean}} \times \text{SlotTime} = 7.5 \times 9 \mu s = 67.5 \mu s. \] (8.16)

With an assumed service type best effort, access category \( AC \ 0 \) applies for which the Arbitration Interframe Space (AIFS) duration is defined to \( T_{\text{AIFS}[0]} = 43 \mu s. \) For given values of \( T_{\text{SIFS}} = 16 \mu s \) and \( T_{\text{ACK}} = 44 \mu s \) and omission of RTS/CTS signaling (\( T_{\text{optional}} = 0 \mu s \)), the transmission duration of one frame exchange computes according to equation (6.14):

\[ T_{\text{transmission}_{\text{1024}}} = T_{\text{AIFS}[0]} + T_{\text{backoff}} + T_{\text{frame}_{\text{1024}}} + T_{\text{SIFS}} + T_{\text{ACK}} = 1598.5 \mu s. \] (8.17)

\[ T_{\text{transmission}_{\text{2048}}} = T_{\text{AIFS}[0]} + T_{\text{backoff}} + T_{\text{frame}_{\text{2048}}} + T_{\text{SIFS}} + T_{\text{ACK}} = 2962.5 \mu s. \] (8.18)

Knowing \( T_{\text{beacon}} \) and \( T_{\text{transmission}} \), the number \( N \) of consecutive transmissions in between two beacon broadcasts can be derived according to equation (6.20) and the idle gap duration \( T_{\text{offset}} \) according to (6.22). Table 8.9 summarizes these analytic results. The difference in user throughput \( TP_{\text{user}} \) for applied packet sizes of 1024 byte for beacon periods of \( \Delta T_{\text{BTT}} = 1024 \) ms and \( \Delta T_{\text{BTT}} = 10.24 \) ms amounts to 5120 kbit/s - 4800 kbit/s = 320 kbit/s, which matched quite well the simulation results from Figure 8.28.

The same holds for packet sizes of \( L_{\text{packet}} = 2048 \) byte, where the difference calculates to 5520 kbit/s - 4800 kbit/s = 720 kbit/s, see Figure 8.29.
Table 8.9: Analytical TP loss due to protected beaconing

<table>
<thead>
<tr>
<th></th>
<th>$T_{\text{beacon}}$ [µs]</th>
<th>$T_{\text{transmission}}$ [µs]</th>
<th>$T_{\text{offset}}$ [µs]</th>
<th>N</th>
<th>$T_{\text{user}}$ [kbit/s]</th>
<th>$\Delta T_{\text{P}}$ [kbit/s]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>$\Delta T_{\text{BTT}}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.24 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1024 ms</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lpacket 1024</td>
<td>196</td>
<td>1598.5</td>
<td>453</td>
<td>6</td>
<td>640</td>
<td>4800</td>
</tr>
<tr>
<td>Lpacket 2048</td>
<td>196</td>
<td>2962.5</td>
<td>1156.5</td>
<td>3</td>
<td>345</td>
<td>4800</td>
</tr>
<tr>
<td>Lpacket 1024</td>
<td>196</td>
<td>283</td>
<td>139</td>
<td>35</td>
<td>3617</td>
<td>28000</td>
</tr>
<tr>
<td>Lpacket 2048</td>
<td>196</td>
<td>431</td>
<td>131</td>
<td>23</td>
<td>2375</td>
<td>36800</td>
</tr>
</tbody>
</table>

The negative impact further scales for larger beacon frames and higher PHY-Modes. The latter is shown by Figure 8.30. It is assumed that receiving stations are settled close to the AP with good link quality so that transmissions take place at 54 Mbit/s. Similar as for transmissions at 6 Mbit/s, transmission durations according to equations (8.10) - (8.18) can be calculated. Due to the more complex modulation scheme, transmission durations for one single frame exchange are reduced by a factor of approximately 10, resulting in $T_{\text{frame,1024}} = 180 \mu s$ and $T_{\text{frame,2048}} = 328 \mu s$. For such short durations, modeling of the backoff duration by its mean value is not appropriate, hence for the following investigation a best-case analysis with $T_{\text{backoff}} = 0 \mu s$ is derived.

![Figure 8.30: Packet 1024/2048 B, PHY-Mode 54 Mbit/s](image-url)
The resulting difference in peak user throughput $TP_{\text{user}}$ for applied packet sizes of $L_{\text{packet}} = 1024 \text{ byte}$ at beacon periods of $\Delta TBTT = 1024 \text{ ms}$ and $\Delta TBTT = 10.24 \text{ ms}$ amounts to $28936 \text{ kbit/s} - 28000 \text{ kbit/s} = 936 \text{ kbit/s}$. For packet sizes $L_{\text{packet}} = 2048 \text{ byte}$, the loss due to beacon protection is even $38000 \text{ kbit/s} - 36800 \text{ kbit/s} = 1200 \text{ kbit/s}$. Again, simulation and analysis match quite well. Table 8.10 summarizes the differences of user throughput caused by protected beacon broadcast. The applied reference value is $\Delta TBTT = \infty$.

### Table 8.10: Simulated TP loss due to protected beaconing

<table>
<thead>
<tr>
<th>$\Delta TBTT$</th>
<th>$\Delta TP_{\text{user}}$ [kbit/s]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PHY-Mode 6 Mbit/s</td>
</tr>
<tr>
<td></td>
<td>$L_{\text{packet}} = 1024$</td>
</tr>
<tr>
<td>10.24 ms (10 TU)</td>
<td>325.4</td>
</tr>
<tr>
<td>51.20 ms (50 TU)</td>
<td>127.2</td>
</tr>
<tr>
<td>102.4 ms (100 TU)</td>
<td>54.5</td>
</tr>
<tr>
<td>307.2 ms (300 TU)</td>
<td>16.6</td>
</tr>
<tr>
<td>512.0 ms (500 TU)</td>
<td>10.0</td>
</tr>
<tr>
<td>1024.0 ms (1000 TU)</td>
<td>3.3</td>
</tr>
<tr>
<td>$\infty$ (reference)</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>PHY-Mode 54 Mbit/s</td>
</tr>
<tr>
<td></td>
<td>$L_{\text{packet}} = 2048$</td>
</tr>
<tr>
<td>10.24 ms (10 TU)</td>
<td>727.9</td>
</tr>
<tr>
<td>51.20 ms (50 TU)</td>
<td>88.6</td>
</tr>
<tr>
<td>102.4 ms (100 TU)</td>
<td>88.6</td>
</tr>
<tr>
<td>307.2 ms (300 TU)</td>
<td>36.1</td>
</tr>
<tr>
<td>512.0 ms (500 TU)</td>
<td>23.0</td>
</tr>
<tr>
<td>1024.0 ms (1000 TU)</td>
<td>6.6</td>
</tr>
<tr>
<td>$\infty$ (reference)</td>
<td>0</td>
</tr>
</tbody>
</table>

### 8.5.1.2 Beacon Adaptation Strategies

The previous section has shown the harmful impact of beaconing with respect to the overall system throughput. Associated stations of the AP may explicitly request for system information with a ProbeRequest message, hence beaconing mainly addresses non-associated stations. If no new station is expected to arrive, a sophisticated control logic such as the Hybrid Information System can order to reduce or even omit beacon transmission. Since HIS is aware of stations approaching the coverage area of an AP, it will duly direct the system to resume beaconing. Further levels of sophistication incorporate a station’s velocity and its predicted distance to the AP in order to realize dynamic adaptation of the applied beacon interval.

---

40 Total abandonment of beacon broadcast is rather theoretical. Proprietary implementations sometimes require a minimum beacon period ($> x*100 \text{ ms}$) to avoid disassociation.
Within Figure 8.31, different beacon adaptation strategies are proposed. Depending on a station’s distance to the reference handover point (a theoretical coverage boundary used as reference point), different beacon intervals are scheduled. Depending on the approaching terminal’s location, velocity, or further parameters, beacon adaptation within the Hot Spot is performed. It is worth mentioning that the approaching station itself does not receive any beacon broadcasts prior to passing the reference HO position. However, Figure 8.31 has illustrative character since real deployments face numerous stations that simultaneously approach the AP. Hence, beacon adaptation is based on their overall distribution justifying the different adaptation strategies.

![Diagram of beacon adaptation strategies](image)

**Figure 8.31: Dynamic Beacon Adaptation**

Dynamic beacon adaptation leads to the idealized case within which only one single beacon is transmitted. HIS hereby controls VHO triggering to the station and beacon transmission by the AP in a coordinated manner. Accordingly, synchronization of the terminal achieved due to well-scheduled (single event) bea-
coning is denoted *Beacon on Demand* (BoD). Besides prevention of signaling overhead, BoD allows for reduced handover latency due to optimal synchronization at the earliest possible stage, cp. Section 8.2.1. Obviously, BoD is only possible for adequate knowledge of actual coverage boundaries. Possible detection methods to be applied such as the Centre of Gravity algorithm have been presented in Chapter 8.3.1.

![Diagram](image.png)

**Figure 8.32: Capacity enhancements due to adaptive beacon control**

Figure 8.32 depicts potentials gains for different applied beacon adaptation strategies. The position of the starting point D = 0 m was chosen according to the reference HO-position that would adjust, if antenna gains were considered. The given example assumes an initial beacon period of $\Delta TBTT = 1024$ ms (1000 TUs) for D = 0 m and $\Delta TBTT = 102.4$ ms (100 TUs) for D > 64 m. Increased beacon intervals applied for distances 0 m < D < 64 m result in increased cell throughput compared to scenarios without beacon adaptation. The resulting potential gain depends on the beacon adaptation strategy and the station’s velocity. Best case profits result in an additional transfer volume of up to 76.8 Mbit (corresponding to the integral of the rectangle potential gain field in Figure 8.32) for a single step strategy with $\Delta TBTT = 1024$ ms $\Rightarrow$ 10.24 ms for slowly moving stations at $v = 1$ m/s.
8.5.2 Directed Beaconing

Previous scenarios assumed terminals approaching the coverage border of a cell. Within the scenario of Figure 8.31, omnidirectional beacon broadcasting was applied for which HIS only needed to coordinate terminal arrival and beacon transmission in the time domain.

Knowing a terminal’s position allows for exploitation of space domain characteristics as well. While the ability to transmit directed beams nowadays is still restricted to professionally used hardware, it is expected that this ability will be supported by SoHo equipment in the near future as well. Inherent antenna gains hence will allow for coverage increase with respect to specific directions. This in turn can be exploited to establish connectivity to approaching terminals much earlier as hitherto, see Figure 8.33 case 1.

In addition, Figure 8.33 case 2 depicts another value added application of HIS controlled system interworking. Assuming a terminal does not approach the coverage area of an AP but is about to pass nearby, ordinary schemes based on scanning would not allow for beneficial VHO. Application of HIS controlled directed beaconing allows for complementary system use even in this case.

![Figure 8.33: Benefits due to directed beaconing](image-url)
It is worth mentioning that neither case 1 nor case 2 could possibly be realized without intervention of sophisticated control logic such as HIS. Having the ability to perform beamforming is pointless without knowledge on time (time domain) and direction (space domain) of operation.

It was shown in Section 8.2.1 that downward vertical handover control from UMTS to WLAN solely based on self-conducted scanning does not allow for optimum handover performance. Depending on the applied beacon interval in WLAN, the scanning interval in UMTS and the velocity of the terminal, detection of and subsequent association to Hot Spots is deferred or even missed. Figure 8.34 shows simulation results for the scenario depicted Figure 8.33. A terminal being connected to UMTS approaches the coverage area of an AP at \( v = 30 \) km/h. A constant bit rate speech service at 64 kbit/s resembling VoIP as described Section 8.1, Table 8.1 is assumed. Due to general user policy, handover to WLAN shall be triggered whenever possible. Without trigger support by HIS, optimum VHO control is delayed as was already shown in Section 8.2.1. Applying HIS control allows optimized complementary system detection by indicating WLAN presence to the user (signaled via UMTS). VHO handover execution is accelerated by further advising the serving AP to perform synchronized beaconing (Beacon on Demand). After successful VHO, the current service is seamlessly continued. Packets that temporarily cannot be delivered during VHO execution are queued and delivering straight after link establishment to the new AP. Ceasing bandwidth constraints even allow for improved quality by doubling user data rate to 128 kbit/s. In addition, a second service is started, streaming in DL direction at 256 kbit/s.

However, the scope of this investigation is not on demonstrating the obvious fact that WLAN supports higher data rates than UMTS. The metric used for evaluation is the distance \( d \) to the AP illustrating earliest possible VHO.

Further benefit is given if antenna gains are exploited. Note that the two cases shown in Figure 8.33 only apply for involvement of a sophisticated control logic. Link state maps as administered by HIS allow for consideration of increased coverage. Based on the terminal’s current position provided while being connected to UMTS, HIS calculates whether coverage would be given for correct antenna adjustment. For positive algorithm outcome, the Beacon on Demand directive to the AP is supplemented by control data indicating the beamforming
direction. This is how HIS controlled VHO enables connectivity that is not supported by conventional schemes that are based on self-conducted scanning.

The solid lines in Figure 8.34 illustrate simulation results for HIS controlled directed beaconing assuming a unidirectional antenna gain of $10 \times \log(g_A) = g_A$ [dB] = 3 dB at either receiving or transmitting side. Enhanced coverage support of up to 255 m in total is given if HIS is applied together with directed antennas. HIS control without antenna gain as indicated by the dashed lines still allows for initial downward VHO at a distance of 191 m from the AP. Without HIS support, VHO applies at an average of 171 m (cp. Section 8.2.1 on delayed system detection due to self-conducted scanning), regardless of the applied antenna type. Since the direction of the approaching terminal is not known, no specific beamforming can be applied.
Simulation results above are inline with analysis. Due to Table 8.5, the minimum receiver sensitivity for BPSK1/2 amounts $P_r = -82$ dBm. Applying the pathloss model from equation (8.8), the resulting coverage calculates by:

$$P_r(d_{max}) = P_s * g_a * \left(\frac{\lambda}{4\pi d_0}\right)^2 \left(\frac{d_0}{d_{max}}\right)^\gamma$$

for $d_0 = 1m, d_{max} > d_0 \quad (8.19)$

$$\Rightarrow \lg \left(\frac{P_r(d_{max})}{P_s \ast g_a \left(\frac{\lambda}{4\pi d_0}\right)^2}\right)^{\frac{1}{\gamma}} = \gamma \ast \lg \left(\frac{d_0}{d_{max}}\right) \quad (8.20)$$

$$\Leftrightarrow \lg (P_r(d_{max}))-\lg (P_s)-\lg (g_a)-2*\lg \left(\frac{\lambda}{4\pi d_0}\right) = \gamma \ast \lg \left(\frac{d_0}{d_{max}}\right) \quad (8.21)$$

$$\Rightarrow d_{max} = 10^{\left(\frac{\lg (P_r(d_{max}))-\lg (P_s)-\lg (g_a)-2*\lg \left(\frac{\lambda}{4\pi d_0}\right)}{\gamma}\right)} \ast d_0 \quad (8.22)$$

For a given pathloss coefficient $\gamma = 2.4$, frequency $f = 5.5$ GHz ($\Rightarrow \lambda \approx 0.0545$ m) and a required receive- and send power $P_r$ and $P_s$ according to equation (8.19),

$$P_r(d_{max}) \ [\text{dBm}] = -82 \ dBm \Rightarrow P_r(d_{max}) = 10^{-82} \ast 1mW = 6.31 \ast 10^{-9} \ mW \quad (8.23)$$

$$\wedge P_s \ [\text{dBm}] = 20 \ dBm \Rightarrow P_s = 10^{20} \ast 1mW = 100.00 \ mW$$

the upper coverage limit $d_{max}$ is given by equation (8.24).
While HIS support in terms of Beacon on Demand with associated beamforming control essentially pays off for terminals *approaching* the coverage area of an AP, no further benefit is given when *leaving*. Figure 8.35 depicts upward VHO (WLAN -> UMTS) occurrence after link lost. The 256 kbit/s streaming service is stopped completely and the 128 kbit/s VoIP service is downgraded back to 64 kbit/s after VHO. Again, directed antennas lead to increased coverage but contrary to the scenario with approaching terminal, application of HIS does not result in superior coverage support.

As a summary, it was shown that HIS allows for increased performance in terms of earliest possible handover support. Particular benefit is given, if applied together with beamforming since this allows for VHO cases (see Figure 8.33) that could not be triggered without HIS involvement. Once VHO to WLAN has taken place, no further coverage gain is given for leaving terminals due to HIS. Table 8.11 provides a comparative summary of the different application cases.

**Table 8.11: Beneficial application of HIS targeting on maximized WLAN coverage**

<table>
<thead>
<tr>
<th>characteristic</th>
<th>HIS &amp; antenna gain</th>
<th>HIS</th>
<th>No HIS &amp; antenna gain</th>
<th>No HIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>approaching</td>
<td>Beacon on Demand &amp; beamforming</td>
<td>Beacon on demand</td>
<td>Self-conducted scanning &amp; beamforming</td>
<td>Self-conducted scanning</td>
</tr>
<tr>
<td>leaving</td>
<td>+</td>
<td>o</td>
<td>+</td>
<td>o</td>
</tr>
</tbody>
</table>

\[
d_{\text{max}} = \left\{ \begin{array}{c} 10^{\frac{10\times\log(0.0545 m)}{10^{4.24}}} \\
10^{\frac{10\times\log(6.31 \times 10^{-6}) - 10\times\log(100) - 20\times\log(\frac{0.0545 m}{4\pi r_{\text{IN}}})}{10^{4.24}}} \\
10^{\frac{10\times\log(6.31 \times 10^{-6}) - 10\times\log(100) - 20\times\log(\frac{0.0545 m}{4\pi r_{\text{IN}}})}{10^{4.24}}} \end{array} \right. \\
*1m = 191m, \text{ no gain} \\
*1m = 255m, \text{ 3dB gain} \\
\]

(8.24)
8.5.2.1 Regulatory Limitations

Regarding coverage extension due to application of beamforming with directed antennas, some regulatory limitations need to be considered. In fact, regulatory authorities do not prescribe maximum coverage areas but define maximum transmission power limitations. More precisely, limitations on the Equivalent Isotropically Radiated Power (EIRP) need to be followed by RF equipment.

\[
EIRP \ [\text{dBm}] = \text{transmit power} \ [\text{dBm}] - \text{pathloss} \ [\text{dB}] + \text{antenna gain} \ [\text{dB}]
\]  

Equation (8.25) gives the definition of EIRP. Antenna gain is expressed relatively to a (theoretical) isotropic reference antenna and considers possible losses from the antenna cable. The EIRP value hence is the amount of power that would have to be emitted by an isotropic antenna that evenly distributes power.
in all directions to produce the peak power density observed in the direction of maximum antenna gain.

Regulatory limitations on an EIRP basis hence imply that if the AP in Figure 8.33 initially transmits omnidirectional beacons with the maximum $T_x$ power, application of directed antennas does not lead to any coverage gain since due to the EIRP ruling the AP needs to reduce the $T_x$ power by the same amount as the antenna gain increases.

Most European countries have joined CEPT's (European Conference of Postal and Telecommunications Administrations) proposition of European harmonization of frequencies for wireless networks. For the 2.4 GHz band, ETSI EN 300 328 [139] defines a maximum EIRP value of 100 dBm ‘for any combination of power level and intended antenna assembly’. For the 5 GHz band, ETSI EN 301 893 [140] defines EIRP values between 20 dBm and 30 dBm, depending on the used sub-band and depending on application of transmit power control.

In the United States, the Federal Communications Commission (FCC) regulates the use of antennas through FCC Part 15.247 [141], which defines power limitations for wireless LANs. When using omnidirectional antennas, a maximum transmit power of up to 1 W is allowed. In contrast to European regulation, FCC relaxes EIRP limitations with higher gain directive antennas. When using antennas having a gain of at least 6 dBi, the FCC allows operation up to 4 W EIRP, which is 1 W plus 6 dB of gain. For antennas with gain greater than 6 dBi, the FCC requires reduction of output power by the amount in dB that the directional gain of the antenna exceeds 6 dBi. Further concession is given to fixed point-to-point deployments: For the 2.4 GHz band, $T_x$ power only needs to be reduced by 1 dB for every 3 dB that the directional antenna exceeds 6 dBi. This means that as antenna gain goes up, $T_x$ power is decreased by less. For the 5 GHz band, the same installation may employ transmitting antennas with directional gain greater than 6 dBi without any corresponding $T_x$ power reduction. The reason why higher EIRPs are acceptable for FCC is that higher gain antennas are more directive, reducing potential interferences with adjacent systems.

Summarizing this, the principle of directed beaconing as proposed in Section 8.5.2 primarily applies in countries with more relaxed EIRP ruling. However, keeping in mind that antenna gains apply for both, transmission and reception, directed beaconing might even be an option in Europe in spite of strict EIRP
regulation. In that case, the terminal also needs to support directed antennas so that coverage extensions as indicated in Figure 8.33 solely are achieved due to antenna gains on the *receiving* side. Up to now, smart antenna techniques are not yet available for handheld devices, but research is going on, e.g., Fujitsu announced smart antennas for mobile terminals [142]. In addition, the emergence of MIMO technologies is expected to serve as further driver for sophisticated antenna technologies for both, stationary devices and mobile terminals.

In any case, the application of adaptive beacon control leads to reduction of interference in the cell. Thus, regardless of the European EIRP legislation, HIS enabled adaptive beaconing provides significant benefits.

### 8.5.2.2 Intermediate Hidden Station

Application of directed beaconing opens up new interesting use cases but introduces scenario specific problems as well. Coverage extensions indicated by $D_{\text{Gain}}$ in Figure 8.36 due to HIS controlled directed transmissions allow for communication with terminal $\text{MT}_A$ residing outside the omnidirectional coverage area $\text{D}_{\text{AP}}$. Since only the AP disposes of directed antennas, communication between AP and $\text{MT}_A$ is possible while $\text{MT}_B$ and $\text{MT}_A$ are not aware each other since their in-between distance $\text{D}_{\text{MT}_B} - \text{D}_{\text{MT}_A}$ exceeds the coverage distance $\text{D}_{\text{cover}}$. From $\text{MT}_A$’s point of view, $\text{MT}_B$ acts as hidden station with respect to transmissions from $\text{MT}_A$ to the AP.

![Figure 8.36: Hidden Station Problem with Adaptive Beaconing](image)

**Figure 8.36: Hidden Station Problem with Adaptive Beaconing**
The interesting fact with this scenario is that the hidden station $MT_B$ resides *in between* the two communicating parties $MT_A$ and AP. However, the problem of hidden stations is well known and the specification offers with the RTS/CTS mechanism a solution to this problem that can also be applied for intermediate hidden stations.
This thesis addresses aspects of system integration and interoperability. The goal is to open up new concepts paving the way towards next generation mobile communications. Based on the assumption that interoperability is a main requirement to be met by future networks, the key challenges to be fulfilled are system cooperation, information exchange, and seamless service continuity. This thesis introduces and elaborates the Hybrid Information System (HIS) as a new framework for inter-system collaboration of heterogeneous mobile radio networks. Particular focus is put on context information in terms of location that is associated with link state information derived from measurement reports. Hence, overarching system control with focus on vertical handover triggering is the primary objective. The need for self-conducted scanning is reduced or is even made obsolete. The integration of system specific information with context (location) data together with providing this bundle as cross-system information produces significant benefits.

There have been exemplary investigations carried out for UMTS and IEEE 802.11(a/h/k), whereas the concept is scalable and allows easy incorporation of further standards. The underlying principles for HIS operation, acquisition of measurements and localization, have been introduced in the beginning of this thesis. A detailed specification of the Hybrid Information System has been provided, complemented by a description of the demand for system integration, as seen by the research community. Feeding, administration, and processing of HIS data are also considered as well as possible application areas. A subsequent discussion on the architecture then addresses the aspects of realization of the proposed concept.

A prototypical HIS implementation was established in the scope of this thesis. Validation of the simulation environment has been ensured for the integrity of the resultant outcomes. Both, analysis and simulation are applied subsequently revealing the potential of overarching system control by HIS.
For the modeling of location errors, it has been demonstrated that stochastic error distributions can be applied to model emerging errors due to non-perfect localization. A two-dimensional Gaussian error distribution with non-correlated deviations in x- and y-direction was applied considering long-term measurements by HIS. The mathematical model needed to be further adjusted to reflect real radio conditions more precisely. In introducing the cut-off criterion, statistical outliers were eliminated while statistical properties of the resulting probe were derived. A correlation analysis, with the correlation coefficient $\rho$ as evaluation criterion, was discussed. Considering real position and erroneous position, it was shown that location data based decision algorithms perform best if the terminal resides close to the cell edge. This is of particular interest for handover control as considered in this thesis. In addition to location aspects, service maintenance has been addressed. It was shown that an integrated system is able to support specific high bit rate services though only partial WLAN coverage is given. Proxy buffering and UMTS based data supply bridge potential connectivity gaps (user plane) and allow session maintenance (control plane) making time consuming re-establishment negotiations obsolete.

The benefits of the Hybrid Information System are shown to be particularly evident in the simulation chapter of this thesis. It is demonstrated that conventional system control approaches based on self-conducted scanning have drawbacks that can be overcome by HIS: For UMTS, application of the compressed mode entails drawbacks with respect to overall system performance. For WLAN, self-conducted scanning resulted in reduced overall throughput due to delayed hot spot detection. HIS based system control overcomes both of these detriments by eliminating the need for self-conducted scanning.

Besides this, HIS entails further potentials for optimizing handover triggering. A new algorithm, the Center of Gravity (CoG), ensures that even in case of erroneous location data best-suited coverage detection of a VHO candidate system is always achieved. Additional benefits result from context information to be provided by HIS together with the handover triggers. This is how link adaptation can be anticipated and accelerated. Finally yet important, another example for HIS based system control is presented within which beaconing is beneficially adjusted for the sake of both, a single terminal and an entire system. Particular benefits are given for joint application with directed antennas. Adaptive beacon control therefore results in the prevention of wasted capacity on the one hand, and facilitates enhanced connectivity on the other hand. The resulting use cases
disclose a huge potential and cannot be realized without the intervention of a sophisticated control logic such as HIS.

**Outlook**
This thesis introduces and elaborates the idea of cooperation of radio access networks using third party location data. Within this work, the raw concept has been developed from its initial stage to a concrete cooperation scheme. A prototypical implementation was achieved testifying the benefits of the proposed concept. Leading IST-projects such as WINNER have taken up the HIS idea making it a promising concept for future networking.

The link state maps administered by HIS represent a worthwhile resource. From a technical perspective, evaluation in the time and space domain is applicable to achieve system optimization and support network planning. The service perspective will put the focus on prediction and profiling. Location based networking along with location based services has raised increasing attention in the recent years and will experience further attraction in the future.

Efficiency considerations require services to be provided by the best-suited system. However, the rising demand for integrated networks, possibly including fixed-mobile convergence as well, requires heterogeneity to be limited. Cooperation and interworking are therefore the overarching solutions. Thereby, the beneficial property of HIS scales up, the more complementary systems need to be interconnected. Since HIS allows incorporation of existing as well as future specifications, it assures smooth migration and sustainability while also leaving scope for further innovation.

Mobile radio systems address two basic human needs: *Communication* and *Mobility*. The contributions of this thesis have the potential to serve as enabling concept for supplying such needs in the face of next generation networks by giving a platform for overarching system control and inter-system information exchange.
HIS: Further Application Areas and Related Work

Content

A.1 Measuring of non-accessible areas .................................................... 285
A.2 ABC Support ..................................................................................... 286
A.3 Radio Resource Management & Connection Admission Control .... 286
A.4 Positioning Support ................................................................. 287
A.5 Location Aware Networking ......................................................... 288
A.6 Navigation Support ........................................................................... 289
A.7 Related Work ..................................................................................... 289

Keywords: HIS Application Areas, HIS related Projects

The Hybrid Information System offers a variety of application areas. Some examples have been presented in Section 5.5 and further elaborated in the analysis and simulation chapters of this thesis. However, a couple of follow up application areas are possible that will be shortly summarized in the following. Beyond the background, that knowledge of link states in the field together with position information is a worthwhile piece of information, the Hybrid Information System has the potential to serve as enabling platform for many new services. At the end of this annex, HIS’ relation to other concepts is shortly discussed.

A.1 Measuring of non-accessible areas

Applying the HIS idea inherently turns each associated terminal into a measurement device – regardless whether the terminal respectively the user is aware of this integration or not. By such, it becomes possible for the operator to gather link information on areas being non-accessible otherwise. Whether private flats, company premises, or office buildings - places that usually cannot be accessed can be measured as long as mobile users roam.
In addition, expenses arising from extra measurement rides can be reduced. Results deriving from HIS databases potentially are more exhaustive due to the large number of feeding clients while at the same time representative since being based on life network conditions.

It is worth mentioning that privacy aspects might be an objection inhibiting this application to be put into practice. In order to address this rather sensitive field, some general remarks with respect to privacy have been taken up in Section 4.1.2.3 in the context of Location Based Services.

A.2 ABC Support

*Always Best Connected* (ABC) is an emerging concept for 4G mobile communication systems. The main task is to offer the opportunity to the user to choose anywhere, anytime, and from any network the best connection regarding QoS requirements, terminal capabilities and characteristics of the available access networks. The ABC concept is encouraged by the existence of multiple access network technologies, emerging multi-mode terminals, and different user service requirements. Due to HIS inherent knowledge about general properties and current link situation of each associated network, respective VHO trigger can be generated. Moreover, trigger generation can also be omitted if for the sake of the user. This could be the case if moving at high velocities or due to user preferences (‘connect to WLAN whenever possible’ or ‘stay connected to 3G networks despite of WLAN technology being available to accommodate needs for increased security’) taken into account by the HIS decision-making process.

A.3 Radio Resource Management & Connection Admission Control

Having detailed information on current position and related link budget allows supporting of associated control entities and algorithms like e.g., RRM. On the one hand, it is possible to perform active load balancing between different types of networks for the sake of both, the user and the operator, on the other hand, exploitation of HIS data in conjunction with intelligent tracking schemes allows prediction of e.g., users’ movements, which subsequently may be used to support planned actions such as handover. If the HIS system informs a possible target AP/BS that a mobile user is likely to handover within the near future, a respective CAC algorithm may consider this when currently assigning resources to other devices or accepting new calls. This is how HIS supports prioritization of
ongoing communication. Handover terminals will face an increased chance for connectionless service improving a system’s *Grade of Service* (GoS).

### A.4 Positioning Support

Serving as central entity within a heterogeneous network environment, HIS disposes of link state information for each associated system in its entire administered geographical area. Speaking in terms of characteristic attributes, each position is uniquely identified by a tuple of receive signal strength indicators. While HIS service engaged in this thesis demands for position related measurements, the other way round applies just as well. It is hence possible to provide measurements to HIS databases in order to figure out the current position:

\[
\text{Position} \rightarrow \text{HIS database} \rightarrow \text{Measurement Report (mainly applied in this thesis),}
\]

\[
\text{Measurement} \rightarrow \text{HIS database} \rightarrow \text{Position.}
\]

As signal levels are not static but subject to ongoing fading impacts, it is usually not sufficient to perform positioning based on *one single* measurement. Hence, a *sequence* of measurements is needed. The variation within measured levels entails further characteristic information. Being mapped against a database that previously has been fed with characteristic pattern and related position information, derivation of one’s current position is possible. Database queries thereby may be implemented in many different ways, e.g., Kennemann [181] has proposed a method being based on Hidden Markov Models (HMM). Reliability of HMM based positioning can be further improved, if the models initially are encoded with well-known training sequences. Mangold et al. [182] have verified the applicability of the HMM-based method in real field trials and it was shown to perform quite well.

While the previously described HMM-approach was applied exclusively to GSM systems, the HIS approach allows for incorporation of heterogeneous system data. The underlying HMM hence becomes a multi-dimensional model. In addition, acquisition of certified training sequences can be managed quite easily but cheap, though, by authorizing only particular feeding clients (e.g., stations being equipped with GPS modules to assure integrity of associated position data) to provide reference input for HIS databases.
A.5 Location Aware Networking

Awareness of link conditions at dedicated positions together with tracking feasibilities as offered by HIS’ Service Control Unit, further application areas are enabled herewith subsumed as Location Aware Networking.

Location Based Services
Properties of Location Based Services (LBS) have already been discussed in Section 4.1.2. LBS realization mainly refers to a special piece of information data to be transmitted to the user either on demand or in a push- or broadcast manner. On consuming this data, the user usually shall be guided to or informed about a nearby location or its properties. HIS’ Service Control Unit along with its property to track station movements may be employed to coordinate precise timing of data delivery. However, LBS relying on HIS trigger does not only comprise the service itself, but also how and which data should be provided. Knowing position and related link condition, HIS may support both, the content provider in selecting adapted information considering e.g., user velocity (pedestrians moving slowly along showcases will be provided other information at higher resolution/quality than motorists will) and the network operator to anticipate the best transmission technique/system.

Location Based Billing/Charging
Considering the fact that support of high bit rates at cell edges requires increased system capacity (particularly for UMTS), new charging models based on the location of the user appear interesting. Hence, if a user requests services requiring high-bandwidths, the HIS approach initially makes sure that the service is delivered by the most suited system. Subsequently, HIS can be employed as information desk showing the user whether cheap or expensive transmission is currently charged. In fact, the ‘Homezone’ concept of O2 Germany applies location-based charging in these days already. Depending on the user’s location, speech services are charged differently. Using a special symbol in the terminal display, the user is indicated whether cheap or ordinary service rates apply. While the Homezone concept geographically is not very accurate and applies on cell level only, HIS may be used to increase accuracy, hence different charging zones within one single cell become feasible. Further enhancements are thinkable if navigation support is added (“You are now at the cell edge, move 100 m to your left and the same service is charged half”).
Location Based Admission
HIS’ ability to support tracking and positioning of users based on measurement reports serves as enabler for allocation of location-based properties. While Location Based Billing applies different charging models subject to the user’s current position, similar assignment of access rights solely based on the user’s whereabouts might be an option. The underlying idea is that a user - once he had rightfully passed an encompassing outer barrier of a specific terrain – is granted further admission simply because he resides at his current position. Possible application examples here could be access to fun rides in leisure parks, usage of ski lifts or access to semi-open WLAN at premises.

A.6 Navigation Support
Classical navigation support in the context of Location Based Services allows for requesting of dedicated facilities, such as closest cash machine and the like. Additional value added HIS services further consider link qualities in the field. Possible application areas here comprise

- Identification of the best location in order to use a specific service,
- Looking for the next area covered by operator XYZ, or
- Finding a nearby Hot Spot offering most spare capacity.

In addition to information provisioning on locations of requested items, guidance support (navigation) can be offered, too. Classical navigation requests allow defining search parameters such as shortest or fastest routing. HIS supported navigation is aware of link conditions in the field and hence can offer further query options e.g., ‘best covered’ or ‘least interfered’ route.

A.7 Related Work
Within Section 5, properties of the Hybrid Information System have been presented. In order to emphasize the novel aspects of HIS, the following section provides a description of related work revealing unique and complementary aspects of this contribution.

A key objective of HIS is exploitation of foreign party gained measurement reports with subsequent disposition to other radio systems. The actual benefit is given by combining acquired measurements with position information. Hence,
Location-aware computing is widely discussed to be one attractor of future heterogeneous wireless networks. The importance of this topic is reflected by more than 20 IST projects being organized in the LOcation Based Services clusTER (LOBSTER) of the 5th and 6th European Framework Programme.

One of those projects called CELLO (CELlular network optimization based on mobile Location) [161] relies on similar kind of input data as the Hybrid Information System, utilizing mobile location information for performance enhancements. Some ideas of CELLO have been taken up by HIS and were further improved; others have newly been developed in the scope of this thesis. Within CELLO, requirements for a Mobile Network Geographic Information System (MGIS) are specified. The MGIS system is supposed to be capable of collecting and storing location-related performance data to be used for Location-aided network Planning (LAP). However, clear focus hereby was improvement of existing deployments. Accordingly, CELLO addresses 2G GSM networks and proposed location aided handover procedures target on horizontal handover optimization. In contrast to this, HIS is not restricted to enhancements of existing 2G/3G mobile networks only, but addresses further aspects of system integration with respect to next generation networks. HIS administered databases do not only provide link state maps of one single radio access system, but perform cross-correlation of heterogeneous deployments, e.g., with respect to system availability. Considering vertical handover hence introduces a new dimension with respect to always best connected that was not covered within CELLO. The outcome of this is that beneficial aspects such as decreased necessity for self-conducted scanning of heterogeneous systems and prevention of negative impacts as caused e.g., by compressed mode application are exclusively investigated in the context of this work. Further distinctions are made up due to applied algorithms and resulting conclusions. For example, CELLO states that location errors in positioning are quite harmful since they may lead to unwanted results, such as handover to nonexistent networks [162]. Contrary to this, HIS introduces with the Centre of Gravity (CoG), see Section 8.3.1, a new method that precisely because of location errors beneficially helps estimating cell borders.
Within the IST LOBSTER cluster, there are further projects that integrate location context in order to facilitate value added services. Details to the following shortly described LOBSTER projects can be found on the respective IST project description homepages of the European Union [163]:

The EMILY (European Mobile Integrated Location sYstems) project aimed on technological development in view of the implementation of efficient location services exploiting terrestrial and satellite location data. Being restricted mainly to hybrid E-OTD/OTDOA and GPS positioning methods, the approach followed was a service oriented product development (new positioning ASICS chipset) with short time to market perspective. Contrary to this, HIS follows a more visionary approach on system integration with respect to current and next generation radio systems.

The WINE GLASS (Wireless IP Network as a Generic Platform for Location Aware Service Support) project focused on location and QoS aware services and applications. Contrary to HIS, radio aspects play a minor role only. Instead, higher layer based macro mobility supported by IP based service platforms has been the focus here.

The U.C.A.N. (Ultra-wideband Concepts for Ad-hoc Networks) project’s main objective has been to provide a generic platform for a self-organizing wireless personal area networks containing high accuracy in-door positioning functionality. The topic of location aware ad hoc networking is out of scope of HIS.

The aim of the LoVEUS (Location aware Visually Enhanced Ubiquitous Services) project has been to design a framework for provision of personalized, tourism-oriented multimedia information related to the user’s location. Considering the LoVEUS framework as infrastructure for third party content providers, the Hybrid Information System could be an enabler concerning the derivation of location information and radio technology selection for service provision.

One further clear distinction to all other discussed projects is the generic and scalable approach followed by the Hybrid Information System. It is worth noting that HIS enabled interworking between different systems as shown in Figure 5.1 and Figure 5.2 is neither restricted to a particular radio system nor does it prescribe a maximum number of participating technologies. The only requirement is that systems to be incorporated into the HIS concept provide measure-
ment reports into HIS’ databases to indicate their current status. Not even positioning is mandatory, if location information to be associated may be derived by means of foreign localization.

More recently, the topic of location aware computing plays a more and more important role within large (integrated) projects of the 6th European Framework Programme. In fact, the Hybrid Information System was taken up and integrated into the WINNER (Wireless World Initiative New Radio) project, where it is an integral part to support cooperation of radio access systems.

In addition to aspects with respect to location-aware computing, the Hybrid Information System further features by system integrative properties. Due to the importance of this topic, related work with respect to heterogeneous networking has been described separately in Section 3.2. Further descriptions of FP6 IPs can be found there as well.
Any service being based on more or less accurate positioning information needs to fall back on appropriate means to delineate a certain area in a one-to-one manner. Accuracy and precision, as described in Section 4.5, aim at describing properties of localization. Hence, these are related pieces of information needed to characterize a specific place more precisely. For the respective place itself, a commonly agreed notation needs to be applied. This shall qualify a position in such a manner that other parties undoubtedly target the same place when applying the same notation.

The scientific discipline that deals with the measurement and representation of Earth and its gravitational field is called Geodesy. Its origin is based on the exigency to parcel out territories, define property lines and document frontiers.

**B.1 Introduction**

Description of positions usually is based on previously agreed reference systems. The most important global model is the Geoid, which is a mathematical figure of Earth. It was firstly described by C.F. Gauss in 1828 and further developed by J.B. Listing who also created this notation in 1872. The Geoid represents the equipotential surface of the Earth's gravity field which best fits, in a least squares sense, global mean sea level [152]. All geodetic altitudes are reported with respect to the Geoid.
For practical reasons, however, the physical Geoid model is mathematically too complex, for which it is only used in special cases. Instead, a mathematically more simple *reference ellipsoid* is defined, which is used in 99% of all cases. The reference ellipsoid is a geometrical model, representing a rotation ellipsoid that fits best with the Geoid. It is used as the surface on which geodetic network computations are performed and point coordinates are calculated.

![Figure 9.1: Geoid with reference ellipsoid](image)

While the Geoid is a *physical* Earth model, the rotation ellipsoid is a *geometrical* model. Mathematically, it is a flattened ellipsoid of revolution with two different axes, an equatorial semi-major axis $a$ and a polar semi-minor axis $b$, see Figure 9.1. The flattening $f$ is defined as

$$f = \frac{a - b}{a} \quad (9.1)$$

and the first eccentricity $e$ by

$$e^2 = \frac{a^2 - b^2}{a^2} = f(2 - f). \quad (9.2)$$

For the Earth, the flattening $f$ is around $1/298$, caused by the Earth's rotation.
B.1. Introduction

Geodetic points on Earth’s surface typically are stated by two polar coordinates: First, the longitude \( \lambda \), which is the angle between the Greenwich Prime Meridian and the meridian of interest, and second the latitude \( \phi \), which denotes the angle between a perpendicular at a location, and the equatorial plane of the Earth, see Figure 9.2. Descriptions of geodetic positions apply degrees (°), arc minutes (') and arc seconds (") for longitude and latitude. A further parameter, altitude \( h \), represents the height over the reference ellipsoid.

Given these coordinates, i.e., latitude \( \phi \), longitude \( \lambda \) and altitude \( h \), one can compute the geocentric rectangular coordinates of a point applying the following transformation:

\[
\begin{align*}
    x &= (N + h) \cos \phi \cos \lambda \\
    y &= (N + h) \cos \phi \sin \lambda \\
    z &= (N(1 - e^2) + h) \sin \phi,
\end{align*}
\]

where

\[
N(\phi) = \frac{a}{\sqrt{1 - e^2 \sin^2 \phi}}
\]

Figure 9.2: Reference ellipsoid (special case: symmetric globe with \( f = e = 0, N = a \))
is the *meridian radius of curvature* of the ellipsoid, \( a \) is the equatorial radius and \( e \) the first eccentricity.

Being a good approximation to the shape of the Geoid and mathematically much more easy to handle, reference ellipsoids are used to provide a figure of the Earth.

However, depending on the level of accuracy to be achieved, one single global reference ellipsoid is not sufficient. Since the shape of the Geoid varies around the globe, different sized ellipsoids have been used for different regions to fit the Geoid as closely as possible. For example, an ellipsoid that provides a good fit of the Geoid over the whole globe is not necessarily the most suitable for North America, and neither would be the most appropriate for Europe. The most important reference ellipsoid for Europe is the Bessel-Ellipsoid (\( a = 6377397.155; 1/f = 299.1528128 \)) defined in 1841 by Friedrich Wilhelm Bessel.

---

![Figure 9.3: Geoid with reference ellipsoids for Europe and North America](image)

The occurrence of regional reference ellipsoids is determined if two of the three parameters, semi-major axis \( a \), polar semi-minor axis \( b \) or flattening \( f \), are known. Further, orientation and position in space need to be specified to assign a well-defined altitude to the model. This is achieved by defining a specific reference point serving as anchor. At the anchor’s position, the Geoid and the applied reference ellipsoid match in a best possible way. Accordingly, regional reference models are non-geocentric.
The combination of both, regionally valid reference model plus reference point, is referred to as geodetic datum. Though two countries may apply the same reference ellipsoid, e.g., the Bessel-Ellipsoid used by Germany and Austria, different reference points (Germany: Rauenberg nearby Potsdam, Austria: Hermannskogel nearby Vienna) are specified to achieve best possible fitting with the Geoid.

In summary, positions may be unambiguously described with the help of well-known reference systems. The Geoid is the most important physical model of Earth. Being too complex, a mathematically much simpler geometric model was conceived, approximating Earth as rotation ellipsoid. There might be one single global reference ellipsoid, or many different ones with regional focus only. For the latter case, well-defined reference/anchor points allow for exact placement of the regional reference ellipsoid with respect to the Geoid. The combination of a specific reference ellipsoid and a specific anchor point is referred to as geodetic datum. Traditional geodetic datums are defined regionally and therefore non-geocentric. An important European reference ellipsoid is the European Datum 1950 (ED50) based on the so-called Hayford Ellipsoid from 1924 \( (a = 6 \, 378 \, 388.0 \, \text{m}, \frac{1}{f} = 297.0 \, \text{m}) \) with its anchor point equal to the position of the south tower of the Frauenkirche in Munich. The most important global geocentric reference ellipsoid is the one defined by the World Geodetic System in 1984 \( (a = 6 \, 378 \, 137.0 \, \text{m}, \frac{1}{f} = 1:298.25722) \). It serves as geodetic basis for the Global Positioning System (GPS).

**B.2 World Geodetic System 1984**

The World Geodetic System 1984 (WGS84) [152] provides a geodetic basis that allows surveying of Earth’s surface and determining the orbits of satellites. It defines further a fixed global reference frame for the Earth, for use in geodesy and navigation.

Efforts to supplement the various national surveying systems began in the 19th century. Up to the 1920s, a series of global ellipsoids of the Earth were derived. However, a unified World Geodetic System became essential in the 1950s for several reasons [154]:

1. **Accurate Positioning**: The need for accurate positions of objects on Earth, such as navigation, surveying, and mapping.
2. **Satellite Navigation**: The development of satellite navigation systems, like GPS, required a global reference system.
3. **Geophysical Studies**: The study of Earth's gravity field and other geophysical parameters needed a common reference.
4. **Earth's Rotation**: The understanding of Earth's rotation changes required a stable reference system.
5. **Global Communication**: The expansion of global communication systems, like radio and telecommunication, necessitated a global coordinate system.

The World Geodetic System 1984 (WGS84) was developed to meet these needs and provides a universal reference system for geodesy, navigation, and related applications.
• International space science and the beginning of astronautics,
• Lack of inter-continental geodetic information,
• Inability of existing large geodetic systems such as European Datum (ED), North American Datum (NAD), and Tokyo Datum (TD) to provide a worldwide geo-data basis, and
• Need for global maps for navigation, aviation and geography.

In the late 1950s, a group of international scientists under the leadership of the US Department of Defense (DoD) started to devise the needed world system. The aim was to develop a global reference ellipsoid to which regionally valid geodetic datums could be referred to in order to establish compatibility between the coordinates of widely separated sites of interest. Efforts resulted in specification of WGS 60. Further refinements lead to new schemes including WGS 64 and WGS 72. In the early 1980s, the need for a new world geodetic system was generally recognized. A new model for improved coverage and accuracy was required. Based on the disposition of new data sources such as satellite radar altimetry, the latest revision, WGS 84 dating from 1984, was defined.

WGS 84 is geocentric and globally consistent within ±1 m. It will be valid up to about 2010. Further, it is the reference system being used for coding of locations by all major specifications such as

• Global Positioning System (GPS),
• 3GPP (GSM & UMTS, TS 23.032 Universal Geographical Area Description, [155]),
• IEEE (802.11k, Location Configuration Information [75]), and
• IETF (RFC 3825, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information, [80]).

B.3 Universal Transverse Mercator

Universal Transverse Mercator (UTM) is a global grid designed to work everywhere except at the poles. It is based on geographic coordinate systems with WGS84 as reference ellipsoid, but a different projection is applied. Thereby, the reference ellipsoid is mapped on a cylinder whose Center of Rotation (CoR) lies in the equatorial plane, Figure 9.4b.
The Earth is divided into 60 zones limited by meridians, each spanning six degrees of longitude. Accordingly, the cylinder is rotated each 6°, putting different meridians in its centre. By such, distortion close to the centric meridian is minimized. Due to increasing discrepancies of the geometrical figures reference ellipsoid and cylinder close to the poles, UTM is only valid for latitudes up to 80° South and 84° North, see Figure 9.4d.

The UTM grid specifies a coordinate system that transfers geographic 3D-coordinates into a single 2D plane for which it is well suited to produce graphical representations in maps. Being isogonic, areas within UTM zones are conformal. A specific point is unambiguously referenced by so-called values of easting (E) and northing (N). Easting describes the distance to the currently valid centric reference meridian and northing is the distance, respectively arc length, of the requested point to the equator. For a full position reference, one needs to state the respective zone identifier, Easting and Northing. An advantage is that quantities are in meters, as opposed to degrees/minutes/seconds that vary in length. This makes UTM convenient since coordinates translate directly into
ground distance. Drawbacks are large error ratio (1:2500), exclusion of Polar Regions and difficulties when working with areas lying across zone boundaries.

Many countries have adopted UTM in recent years. Typical there is an old national legacy grid system and a new one based on UTM. Germany used to apply Gauss-Krueger coordinates as described in the next section. Today, GPS-Tools can be used to convert between different coordinate systems.

### B.4 Gauss-Krueger Coordinate System

The Gauss-Krueger coordinate system is a coordinate system that is used for measuring points on the surface of the Earth. The system is named after Carl Friedrich Gauss and Johann Heinrich Louis Krueger and is primarily used in German-speaking countries.

Similar to UTM, it is a grid system that provides a conformable mapping of geographic longitude and latitude position descriptions to planar coordinates. However, corresponding zones as enclosed by two edging meridians do not span six degrees of longitude but three degrees only. The centric median in the middle takes over the same tasks as within UTM: It serves as reference with respect to which the easting is determined. Northing is reported as distance to the equator, just as in UTM.

Though being based on the same mathematical model, the underlying reference system differs between UTM and Gauss-Krueger: While the first applies WGS84 with its globally valid reference ellipsoid, Gauss-Krueger falls back to a regionally valid ellipsoid. For Germany, this is the Bessel-Ellipsoid.

![Figure 9.5: Definition of reference grids for Germany](image)[202]
Figure 9.5 illustrates the Gauss-Krueger the UTM reference grids for Germany. However, in the framework of globalization, the Gauss-Krueger coordinate system more and more is replaced by the UTM coordinate system. Nonetheless, many maps, atlases and official surveying documents are still in use for which it will take another couple of years before entire replacement. Even current mobile radio systems like GSM/GPRS still deploy the traditional system, e.g., O2 Germany applies Gauss-Krueger coordinates to run its location-based ‘Homezone’ service.

So far, the most important reference systems for description of positions have been introduced. Figure 9.6 exemplarily depicts position information for the Chair of Communication Networks, Kopernikusstrasse 16, in Aachen/Germany, together with position information according to WGS84, UTM and Gauss-Krueger coordinates.

**Figure 9.6: Location of Chair of Communication Networks (ComNets)**
APPENDIX C

Specific Measurements in 802.11k

Content

C.1 Channel Load Report...............................................................307
C.2 Noise Histogram Report............................................................308
C.3 Beacon Report.........................................................................308
C.4 Frame Report...........................................................................310
C.5 Hidden Station Report.................................................................311
C.6 Medium Sensing Time Histogram Report.................................312
C.7 STA Statistics Report.................................................................314
C.8 LCI Report................................................................................316
C.9 Measurement Pause Request....................................................317

Keywords: Radio Measurements, Link Conditions, Statistic Information, Status Reports

In addition to spectrum management support by 802.11h, additional procedures are currently specified by 802.11k to support radio measurements. The main target thereby is to provide means for measurement information exchange between different communication partners and third parties. Thus, sophisticated controlling mechanisms and new services shall be supported or enabled.

Radio resource measurement as introduced by 802.11k\(^{41}\) defines some further new Information Elements (=optional components or variable length fields transmitted in the frame body of Management frames, see Section 2.2.4.1). An overview of all IE of 802.11k together with a short explanation is given in Table 9.1.

\(^{41}\) While 802.11h has already been approved, 802.11k is still subject to change. All information and figures compiled for this thesis refer to the latest available draft while writing, which is IEEE 802.11k/D2.0 from February 2005.
Some IEs such as AP Channel Report, Neighbor Report and RCPI have been newly introduced in 802.11k. Their main objective is to provide support in fast and reliable neighbor BSS transition (handover). Being periodically transmitted together with the Beacon, the *AP Channel Report* allows for easy recognition of other APs. More detailed information may be inquired by a STA using a *Neighbor Report Request*. Specific elements included in the response give information whether a new candidate transmission AP supports pre-authentication for fast roaming as specified in 802.11i and indicate whether the new AP supports the same security level as the current one. Further selected capability information deplete the necessity for extra Probe Requests with capability enquiry to each of the reported APs. Once a handover to another AP was triggered, the procedure can be optimized be taking advantage of the Time Synchronization Function (TSF) parameters included in the Neighbor Report. Since the Neighbor Report can also be conveyed in a piggy-backed way with an *Association Response*, all important information on neighbor APs are delivered straight away as soon as a STA associates with an AP. In such a manner, fast proceeding handover as required when traversing adjacent Hot Spots may be facilitated.

However, similarly to 802.11h, 802.11k stresses one particular information element, which is the *Measurement Request/Report* (MR). In addition to the three 802.11h measurement types (Basic, CCA, RPI Request/Report), nine further measurement request types and eight respective responses have been specified: *Channel Load Request/Report, Noise Histogram Request/Report, Beacon Request/Report, Frame Request/Report, Hidden Node Request/Report, Medium Sensing Time Histogram Request/Report, STA Statistics Request/Report, LCI Request/Report and Measurement Pause Request*, cp. Tables 7 in Figure 2.19 and Figure 2.20.

<table>
<thead>
<tr>
<th>Octets:</th>
<th>Channel Number</th>
<th>Regulatory Class</th>
<th>Randomization Interval</th>
<th>Measurement Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Figure 9.7: Generic Measurement Request field for 802.11k measurement types**
Table 9.1: Supported IEs for spectrum management in 802.11k

<table>
<thead>
<tr>
<th>Information Element (IE)</th>
<th>Element ID</th>
<th>Provided Information/Purpose</th>
<th>Used in subtype frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEs in 802.11 (legacy)</td>
<td>0 - 31</td>
<td>see [67], Table 20</td>
<td></td>
</tr>
<tr>
<td>Request Information</td>
<td>10</td>
<td>Means to explicitly request/provide any other Information Elements (e.g., from Table 2.7, or in this table)</td>
<td>Probe Request, Probe Response, Association Request/Response (only neighbor report = IE 52)</td>
</tr>
<tr>
<td>(specified in 802.11d adapted by 802.11k)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEs in 802.11h</td>
<td>32-41</td>
<td>see Table 2.7</td>
<td></td>
</tr>
<tr>
<td>Measurement Request</td>
<td>38</td>
<td>Channel Load Request, Noise Histogram Request, Beacon Request, Frame Request, Hidden Station Request, Medium Sensing Time Histogram Request, STA Statistics Request, LCI Request, Measurement Pause Request</td>
<td>Action frame (\rightarrow) Measurement Request</td>
</tr>
<tr>
<td>(specified in 802.11h, adapted by 802.11k)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(specified in 802.11h, adapted by 802.11k)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP Channel Report</td>
<td>51</td>
<td>List of channels where a STA is likely to find another AP</td>
<td>Beacon frame, Probe Response frame</td>
</tr>
<tr>
<td>Neighbor Report</td>
<td>52</td>
<td>Specific information on neighbor APs including BSSID information (pre-authentication option, security support, selected capability information), Channel Number, PHY type and synchronization support (TSF Offset, Beacon Interval)</td>
<td>With prior request: Action frame (\rightarrow) Neighbor Report Response, Association Response</td>
</tr>
<tr>
<td>RCPI</td>
<td>53</td>
<td>Reports received channel power of previously received frame ((\rightarrow) active scanning support)</td>
<td>Association Response, Reassociation Response</td>
</tr>
<tr>
<td>Reserved</td>
<td>54-255</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Similar to 802.11h, most of the different measurement type requests in 802.11k apply a generic request field as shown in Figure 9.7. The fields *Channel Number* and *Measurement Duration* have the same meaning as explained for Figure 2.22. A new field, the *Regulatory Class* allows to request/report measurements for different frequency bands. The *Measurement Start Time* field in Figure 2.22 that allows 802.11h to schedule measurement procedures at a dedicated point of time in the future (±32 µs) was replaced by a *Randomization Interval* field in 802.11k. Prior to making any measurements, a STA shall calculate a random delay distributed uniformly in the range of 0 and the randomization interval. The maximum possible value corresponds to $D_{\text{max}} = 2^{16} - 1$ TUs $\approx 67$ s. The new approach for directing measurements by a randomization interval rather than a given time point is beneficial due to several reasons: First, traffic storms that could arise from synchronized broadcast and multicast measurements shall be avoided. Second, reliable measurements can only be derived if being based on statistical independence among probes. Third, it is intuitively senseless to provide means for requesting measures that are to be taken too far in the future (the address room of 64 bit for the Measurement Start Time in 802.11h theoretically allows for scheduling of measurement procedures up to $T_{\text{MST}} = (2^{64} - 1)$ µs $> 500$ years (!) in advance. Thus, replacement of the 8 octet *Measurement Start Time* field by a 2 octet *Randomization Interval* field improves straightforwardness and reduces the overhead.

Anyway, while the Measurement Start Time field in 802.11k was simplified compared to 802.11h, the corresponding *response* frames maintain a similar 8 octet date field to allow for absolute indication of the *Actual Measurement Start Time* at which the reported measurements were taken.

One further innovation of 802.11k is the definition of a *Duration Mandatory* bit-field as shown in Table 6 of Figure 2.19. If set to 1, the specified *Measurement Duration* in Figure 9.7 shall be interpreted as mandatory otherwise it shall be interpreted as target duration.

The following subsections introduce all new measurement types as defined in 802.11k, cp. Tables 7 in Figure 2.19 and Figure 2.20. Most of them apply the generic request format of Figure 9.7, hence, only the corresponding responses are presented. If necessary, additional information on requests formats different to the generic one are described as well. All requests are transmitted in the *Measurement Request* field as shown in Table 5 of Figure 2.19. Corresponding responses are transmitted in the respective *Measurement Report* fields of Table 5 in Figure 2.20.
C.1 Channel Load Report

A Channel Load Report is generated as a reply to a previous Channel Load Request. The request applies the generic format of Figure 9.7, while the report follows the scheme as depicted in Figure 9.8. The first four fields, Channel Number, Regulatory Class, Actual Measurement Start Time and Measurement Duration include likewise information as explained for the request. In fact, if a STA was able to fulfil all requirements as specified, these fields will entail a copy of the preceding request. Similarly, possible differences from requested parameters can be reported.

![Figure 9.8: Measurement Report field format for a Channel Load Report in 802.11k](image)

The actual payload of interest is the Channel Load field. It contains the proportion of measurement duration for which the measuring STA determined the channel to be busy. Following the definition for 802.11h’s CCA Report, the channel load value is defined as:

\[
\text{Channel Load} = \text{Ceiling} \left[ 255 \times \frac{\text{Channel busy time (µs)}}{1024 \times \text{Measurement duration (TUs)}} \right] \tag{9.5}
\]

The Channel busy time in equation (9.5) is the time during which either the physical carrier sense or the Network Allocation Vector (NAV) indicated channel busy.

The difference between the CCA Report in 802.11h, see Section 2.2.5.2, and the Channel Load Report in 802.11k is that the latter comprises both, physical carrier sense mechanisms (Clear Channel Assessment) as well as virtual carrier-sense mechanisms (Network Allocation Vector). In other words, the CCA Report is inherently included in the Channel Load Report.
The need for the definition of the Channel Load Report is easier to understand with an example: A scheduling algorithm that solely exploits 802.11h CCA Reports could easily degrade the overall performance within a scenario. Assuming hidden stations, a CCA Report would report an idle medium. However, a Channel Load Report further considers NAVs as set by the MAC due to RTS/CTS messages. The scheduling algorithms thus would backoff the own medium access so that other transmissions are not disturbed.

C.2 Noise Histogram Report

On accepting a Noise Histogram Request with the generic format as shown in Figure 9.7, a STA shall reply with a Noise Histogram Report according to Figure 9.9. The first four fields are likewise to the ones explained before.

![Figure 9.9: Measurement Report field format for a Noise Histogram Report in 802.11k](image)

The actual payload is reported as Noise Histogram reflected by the eight density fields in Figure 9.9. Compilation of the density histogram resembles the procedure of the Receive Power Indication (RPI) Histogram as defined in 802.11h, see Section 2.2.5.3. Similarly, the same classification as in Table 2.8 is applied for the quantization into 8 density levels. However, while for the RPI Histogram any received power during the whole measurement duration is recorded, the Noise Histogram is based on measurements taken exclusively when NAV is equal to 0. Thus, measurements are only taken when the virtual carrier sense mechanism indicated idle channel. This is how the Noise Histogram Report shall include only non-802.11 energy in its result.

C.3 Beacon Report

On accepting a Beacon Request, A STA shall respond with a Beacon Report for each requested BSSID. The format of the Beacon Request, Figure 9.10, is
slightly enhanced compared to the generic measurement frame format as shown in Figure 9.7. While the first 4 fields are the same, five additional fields have been specified: Measurement Mode, BSSID, Reporting Condition, Threshold/Offset and Hysteresis.

![Figure 9.10: Measurement Request field format for a Beacon Request in 802.11k](image)

The aim of a Beacon Request/Report is to gather information on other BSS in the reception range of a station. The Measurement Mode field in the request indicates the mode to be used for the measurements:

**Passive Mode:** A STA is ordered to compile a report based on all Beacon or Probe Response management frames with the requested BSSID being received within a given time span.

**Active Mode:** The STA is ordered to transmit a Probe Request to the broadcast destination address. The rest of the procedure resembles the passive mode above. Similarities to the active scanning procedure as described in Section 2.2.3.2 are obvious. The difference is that Beacon Request/Reports evaluate both, Beacons and Probe Responses, while active scanning restricts to Probe Responses.

**Beacon Table:** The STA is advised to return a Beacon Report containing the current contents of any stored beacon information for any channel with the requested BSSID. In particular, no extra measurements shall be performed.

The last three fields finally, Reporting Condition, Threshold/Offset and Hysteresis, are used if conditional reporting is to be supported. In this case, no time bounded measurement durations determine the time for feedback signaling. Instead, upper and lower limits for RSSI and/or RCPI are defined. Exceeding or falling below these thresholds initiates the report.
The format of the Beacon Report is illustrated in Figure 9.11. Besides well-known fields as included in all other reports further information fields are included summarizing results of measurements: The *PHY Type* field indicates the physical medium type of the beacon/probe response frame being reported and *RCPI* indicates the channel power with which it was received. *Parent TSF* contains the lower 4-octets of the measuring STA’s TSF timer value at the time the Beacon/Response frame being reported was received. *Target TSF*, in turn, contains the timestamp field from the reported Beacon/Probe Response frame. Further information which were reported within the received Beacon/Probe Response frame are mapped to the *Beacon Interval* and *Capability Information* fields. Any other elements that were received may be reported by the *Received Elements* field.

### C.4 Frame Report

A *Frame Request* frame conveyed with the generic format as presented in Figure 9.7 yields to the compilation of a *Frame Report* frame according to Figure 9.12. Central element here is the *Frame Report Entry* with its four subfields *Transmit Address, BSSID, RCPI* and *Number of Frames*. A Frame Report Entry thus is a summary of the traffic from one specific transmit address, whereby the RCPI indicates the received channel power in dBm. Its value corresponds either to the most recently received frame, respectively is calculated as average of the values of the individual frames received. The *Number of Frames* field is a count of the individual frames transmitted by one specific station and gives information about the activity of this station within the measurement duration.
C.5 Hidden Station Report

Similar to most other radio measurement requests in 802.11k, the Hidden Node Request applies the generic measurement request format in Figure 9.7. If a station accepts a respective request, it shall respond with a Measurement Report frame according to Figure 9.13 containing a variable number of Hidden Station Entries. Each Hidden Station Entry comprises one doublet reporting the MAC address of a hidden station and the number of associated detected frames.

The algorithm to detect a possible hidden station relies on reception of a particular frame transmitted from any Station A to any other Station B. If Station B is supposed to acknowledge the correct reception to Station A, but this acknowledgement cannot be detected by the measuring station, Station B is likely to be a hidden station with respect to the measuring station. Accordingly, the MAC address of Station B, which is known from the initial transmission from Station A to Station B, is recorded as Hidden Station Address. To minimize false alarms,
the measuring station only exploits initial transmissions. Re-transmissions are not evaluated.

C.6 Medium Sensing Time Histogram Report

Similar to the Beacon Request, the Medium Sensing Time Histogram Request (MSTH Request) specifies further request elements in addition to the generic request format from Figure 9.7. The entire format of the MSTH Request element is shown in Figure 9.14.

![Medium Sensing Time Histogram Request Format](image)

Figure 9.14: Measurement Request field format for a MSTH Request in 802.11k

The new elements defined are the Medium Sensing Measurement Subtype, RPI Threshold, Bin Offset, Bin Duration and Number of Bins. The Medium Sensing Measurement Subtype field is used to distinguish further subtypes as presented in Table 9.2.

<table>
<thead>
<tr>
<th>Medium Sensing Measurement Subtype</th>
<th>Medium Sensing Measurement Name</th>
<th>Medium Sensing Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>RPI Time Histogram</td>
<td>Time interval during which RPI is above the specified RPI Threshold</td>
</tr>
<tr>
<td>1</td>
<td>CCA Idle Time Histogram</td>
<td>CCA Idle Time interval</td>
</tr>
<tr>
<td>2</td>
<td>CCA Busy Time Histogram</td>
<td>CCA Busy Time interval</td>
</tr>
<tr>
<td>3</td>
<td>NAV Busy Time Histogram</td>
<td>Initial NAV time value when set</td>
</tr>
<tr>
<td>4-255</td>
<td>reserved</td>
<td>reserved</td>
</tr>
</tbody>
</table>
The general purpose of all Time Histograms is to provide additional information with respect to channel usage rather than sole percentage values of busy or idle time. The CCA report (see Section 2.2.5.2) and the RPI histogram report (Section 2.2.5.3) as specified in 802.11h, for instance, provide feedback on the proportional appearance of busy time or RPI levels within the measurement period. A value of e.g., 50% busy time however entails different possibilities: E.g., a channel was completely busy during the first half of scanning and completely idle during the second half, or a channel is alternately busy and idle with intervals much smaller than the measurement duration. Obviously, information on the respective distribution is lost if only percentage values are provided.

Medium Sensing Time Histograms take this into account by providing information about specific durations, e.g., busy and idle times, represented as probability densities. Information transfer thereby is accomplished with the help of so called Bins. A Bin represents a certain amount of time. The minimum medium sensing interval, Bin 0, is specified by the Bin Offset, see Figure 9.14 and Figure 9.15. Medium sensing intervals smaller than Bin Offset are ignored and not reported. With increasing ordinal number, the time span represented by Bin 1, Bin 2, Bin 3,…, Bin (N-1) increases by Bin Duration, see equation (9.6), whereby N denotes the overall Number of Bins.

\[
\begin{align*}
Bin 0 & = Bin Offset; \\
Bin 1 & = Bin 0 + Bin Duration; \\
Bin 2 & = Bin 1 + Bin Duration = Bin 0 + 2*Bin Duration \\
\vdots & \\
Bin N-1 & = Bin 0 + (N-1)*Bin Duration
\end{align*}
\]

On accepting an MSTH Request, a station is supposed to reply with a MSTH Report according to Figure 9.15. A new field, the Total Number of Medium Sensing Intervals is included for the purpose of assessing the reported data.
Figure 9.15: Measurement Report field format for a MSTH Report in 802.11k

Reliable information on the statistical distribution of channel allocation is a powerful means to support quality of service aspects. The specification of 802.11k [75] proposes to use MSTHs to estimate traffic load priorities or detect non-802.11 radio activities. Knowing the characteristics of another interference source may be exploited e.g., by choosing optimal frame lengths when operating in the same channel.

C.7 STA Statistics Report

A STA Statistics Report is passed back as reply to a preceding STA Statistics Request, see Figure 9.16. Each AP/STA in 802.11 administers a Management Information Base (MIB) that comprises the managed objects, attributes, actions, and notifications required to manage a station. Specific MAC counters administered by the MIB provide the necessary support for access control, generation, and verification of frame check sequences, and proper delivery of valid data to upper layers.
The STA Statistics Report allows providing of information of dedicated so called Group Identities to other stations. The current 802.11k\textsuperscript{42} draft specifies only one Group Identity that basically subsumes all MAC counters. The STA Statistics Report thereby reports incrementally, listing the change in STA counters within the Measurement Duration. A Measurement Duration equal to 0 is used to report instantaneous values of indicated STA counters.

\textbf{Figure 9.16: STA Statistics Request in 802.11k}

\textbf{Figure 9.17: Measurement Report field for a STA Statistics Report & Group Identity in 802.11k}

\textsuperscript{42} All information and figures compiled for this thesis refer to the latest available draft while writing, which is IEEE 802.11k/D2.0 from February 2005.
C.8 LCI Report

The Location Configuration Information (LCI) Report is used to convey information on specific positions of stations. Its format has been adopted from IETF RFC 3825 [80] that specifies an DHCP option for coordinate-based location configuration information. The report includes an LCI element as shown in Figure 9.18 to provide information on latitude, longitude and altitude. Each measure is further characterized by a resolution field. The Datum field comprises an eight-bit value encoding the horizontal and vertical references used for the coordinates given in the LCI. A value of 1 relates to the World Geodetic System 1984 (WGS84), cp. Annex B.2.

![Diagram of Location Configuration Information element in 802.11k]

Figure 9.18: Location Configuration Information element in 802.11k

The mechanism based on which location information to be included in the LCI report is collected is not specified by 802.11k to allow the accuracy of the reported location to be ‘best effort’. A requesting Station A has two options when asking for a position: It may prompt another Station B to provide either the local position (= position of Station A) or it may prompt Station B to provide the remote position (= position of Station B), see Figure 9.19.
In such a manner, a station may derive information on its own position, without any further capability to perform positioning. If the associated AP supports network-based foreign-positioning, the requesting station simply needs to send a local LCI request to the AP.

More information on terminal based, network based, self- and remote positioning is given in Section 4, ‘Localization Techniques & Principles’. The Hybrid Information System as introduced in Section 5 essentially relies on the capability of mobile radio systems to provide measurement reports and location information. With the introduction of 802.11h and k, both, means for deriving measurements as well as for reporting them, are available.

**C.9 Measurement Pause Request**

The *Measurement Pause Request* as shown in Figure 9.20 is the latest measurement request element that has been specified by 802.11k so far. It is used to provide time delays between the execution times of measurement request elements in a Measurement Request Frame. Unlike for all other requests, there is no associated response defined. The only element conveyed is a two octet *Pause Time* field. Bit 0 serves as switch for the time span defined by the remaining 15 Bits. A scale factor of 1 or 1000 corresponding to a minimum/maximum measurement pause duration of $1\text{ms} \leq T_{P1} \leq \approx 33.6\text{s}$ or $1\text{s} \leq T_{P2} \leq \approx 9\text{h} 19\text{m}$ is possible.
Figure 9.20: Measurement Pause Request field format in 802.11k
LIST OF FIGURES

Figure 2.1: UTRA architecture of the access stratum .......................................................... 8
Figure 2.2: UTRA protocol stack at Uu [157] ...................................................................... 9
Figure 2.3: General UMTS Frame Structure for TDD and FDD ........................................ 10
Figure 2.4: Multiple Access in UTRA-FDD [157] ................................................................ 11
Figure 2.5: Multiple Access in UTRA-TDD [157] ............................................................. 12
Figure 2.6: Synchronization and Scrambling Code Detection in UTRA-FDD...................... 15
Figure 2.7: Primary and Secondary Synchronization Channel in UTRA-FDD/-TDD... 18
Figure 2.8: Compressed Mode transmission in UTRA-FDD ............................................... 21
Figure 2.9: Idle mode cell selection & re-selection with economy potential ....................... 23
Figure 2.10: Interfaces with the Physical Layer [64]............................................................ 24
Figure 2.11: Measurement Report procedure in UMTS ..................................................... 29
Figure 2.12: ISO/OSI reference model [84] and IEEE 802.11 [86]...................................... 31
Figure 2.13: Basic access method of legacy 802.11 ........................................................... 32
Figure 2.14: Overview of 802.11 activities ........................................................................ 37
Figure 2.15: Target and actual Beacon transmission on a busy network ......................... 38
Figure 2.16: Passive scanning in 802.11 ............................................................................. 40
Figure 2.17: Active Scanning in 802.11 ............................................................................. 42
Figure 2.18: MAC frame formats in 802.11 ...................................................................... 46
Figure 2.19: Action Frame Format with Measurement Request ......................................... 47
Figure 2.20: Action Frame Format with Measurement Report .......................................... 48
Figure 2.21: Information flow for measurements in 802.11h,k ........................................... 50
Figure 2.22: Generic Measurement Request field for all 802.11h measurement types.. 53
Figure 2.23: Measurement Report field of type Basic report .......................................... 54
Figure 2.24: Measurement Report field of type CCA report ............................................ 54
Figure 2.25: Measurement Report field of type RPI histogram report ............................... 55

Figure 3.1: Development towards 4G .................................................................................. 58
Figure 3.2: Degree of coupling in function of WLAN attachment point [20] ................. 60
Figure 3.3: Projects technologies integration effort ............................................................. 72
Figure 3.4: Control and management integration in heterogeneous technologies .......... 73
Figure 3.5: Technology integration level and handover classifications .............................. 75
Figure 3.6: Efforts on adaptability and reconfigurability.................................................... 76
Figure 3.7: Main components in communication and mobility types............................... 77
Figure 3.8: Mobility aspects in this thesis ......................................................................... 80
Figure 3.9: Terminal Mobility resulting in Handover ..................................................... 82
Figure 3.10: Different HO Types; exemplary for GERAN and UTRAN .......................... 85
Figure 3.11: Connection States for Hard- and Soft Handover ....................................... 88
Figure 3.12: Horizontal and Vertical Handover ............................................................ 92
Figure 3.13: L2 triggering and HO decision as discussed in WINNER [112] ................. 97
Figure 3.14: Policy based trigger generation considering user preferences .................. 99

Figure 4.1: Consumer disposition to spend money on value added services ................ 106
Figure 4.2: Localization based on Cell Identification .................................................... 117
Figure 4.3: Positioning based on signal strength .......................................................... 118
Figure 4.4: TOA positioning in synchronized networks .............................................. 121
Figure 4.5: TDOA resulting in hyperbolic lines of constant differences ...................... 122
Figure 4.6: Addressed area by TA localization .............................................................. 123
Figure 4.7: AoA positioning based on incident angle ................................................... 124
Figure 4.8: GPS positioning based on trilateration ..................................................... 128
Figure 4.9: Terrestrial DGPS principle ........................................................................ 131
Figure 4.10: Aspects of accuracy & precision and mutual interdependency ................ 135

Figure 5.1: Gathering & exchange of HO info data between systems ......................... 142
Figure 5.2: Feeding, administration and supply of data within HIS .............................. 143
Figure 5.3: Data Administration and Service Control within HIS ............................... 144
Figure 5.4: Possible storage of measurement reports inside HIS ................................. 147
Figure 5.5: LCS specification development and status ............................................... 154
Figure 5.6: Integration of HIS into 3GPP LCS network architecture ........................... 157
Figure 5.7: Location Service functions and relation to HIS ......................................... 161
Figure 5.8: HIS with reference model for WLAN access to 3GPP services ............... 165
Figure 5.9: WINNER Logical Node Architecture and relation to HIS ....................... 167
Figure 5.10: Mapping of different system architecture aspects to HIS ....................... 169

Figure 6.1: Modeling of location imprecision based on error distributions ............... 173
Figure 6.2: Measurements at real (A) and erroneous (B) position ............................... 174
Figure 6.3: Measurements at real (A) and erroneous (B) positions ...................... 174
Figure 6.4: Distance related correlation $r_{X,Y}$ and $c_{X,Y}$ for $n$ samples per step ....... 177
Figure 6.5: One dimensional Normal Distribution with cut-off .................................. 178
Figure 6.6: Distribution of measurements for cut-off application ............................. 180
Figure 6.7: Total error distribution without cut-off and cut-off at 20 m ..................... 181
Figure 6.8: Distance dependent correlation $c_{x,y}$ with cut-off thresholds ................. 181
Figure 6.9: Virtually increased Cell Size using Buffering ......................................... 183
Figure 6.10: Transmission and Reception Buffers for virtual coverage .................... 183
Figure 6.11: Idle gaps due to beacon protection ....................................................... 186
### List of Figures

| Figure 7.1: Coupling of Simulation Environments and Extended HIS | 193 |
| Figure 7.2: S-WARP Simulator Structure | 195 |
| Figure 7.3: Structure of the UMTS Simulator URIS | 197 |
| Figure 7.4: URIS Simulator Structure | 198 |
| Figure 7.5: HIS internal setup and decision finding process | 201 |
| Figure 7.6: Extended Hybrid Information System | 203 |
| Figure 7.7: Context Transfer between UMTS and 802.11 | 204 |
| Figure 7.8: VHO Procedure | 206 |
| Figure 7.9: Module Loader Concept | 208 |
| Figure 7.10: Simulator validation scenario | 210 |
| Figure 7.11: Throughput and Queue Length for VHO | 211 |
| Figure 7.12: Queue length & packet delay during VHO for different velocities $v_1$-$v_5$ | 212 |
| Figure 7.13: Classification of VHO as queuing system D/G/1-FCFS | 213 |
| Figure 7.14: Validation of measurements according to 802.11h | 216 |

| Figure 8.1: System detection for different scanning intervals and velocities | 225 |
| Figure 8.2: Simulation scenario for compressed mode analysis | 228 |
| Figure 8.3: Interference increase due to DL Compressed Mode application | 230 |
| Figure 8.4: Simulation Scenario with evaluated- and eight interfering cells | 231 |
| Figure 8.5: Power deviation due to CM application | 233 |
| Figure 8.6: Binary reception model with reference coverage boundary | 236 |
| Figure 8.7: RPI levels and reference sensitivities for PHY-Modes | 238 |
| Figure 8.8: Centre of Gravity Algorithm | 240 |
| Figure 8.9: Coverage detection scenario and results for exact positioning | 242 |
| Figure 8.10: Visualization of HIS DB entries for exact and erroneous positioning | 244 |
| Figure 8.11: Distance $d_{CoG}$ to CoG | 245 |
| Figure 8.12: Distance $d_{CoG}$ to CoG cut along x-Axis, $y = 500$ m | 245 |
| Figure 8.13: Characteristic curve for CoG cell border detection | 246 |
| Figure 8.14: CoG Simulation Scenario | 248 |
| Figure 8.15: Distribution of VHO trigger distances for different CoG thresholds | 249 |
| Figure 8.16: CDF of VHO trigger distances for different measurement densities | 250 |
| Figure 8.17: CDF of VHO triggers distance for different localization errors | 251 |
| Figure 8.18: Windowed Link Adaptation Algorithm (based on [70]) | 253 |
| Figure 8.19: Dynamicity of Link Adaptation | 255 |
| Figure 8.20: Handover Scenario | 256 |
| Figure 8.21: Corresponding long-term data | 256 |
| Figure 8.22: Impact of initial PHY-Mode selection on achieved throughput | 257 |
| Figure 8.23: Scenario Evaluation of Throughput Loss | 259 |
| Figure 8.24: Decrease of System Capacity due to lower PHY-Modes (illustrative) | 259 |
| Figure 8.25: System Throughput (DL) | 261 |
| Figure 8.26: System Throughput (UL) | 261 |
| Figure 8.27: Saturation throughput with BPSK $\frac{1}{2}$ dependent on packet size | 264 |
Figure 8.28: Packet 1024 B, PHY-Mode 6 Mbit/s........................................................... 265
Figure 8.29: Packet 2048 B, PHY-Mode 6 Mbit/s........................................................... 265
Figure 8.30: Packet 1024/2048 B, PHY-Mode 54 Mbit/s............................................. 268
Figure 8.31: Dynamic Beacon Adaptation....................................................................... 270
Figure 8.32: Capacity enhancements due to adaptive beacon control ....................... 271
Figure 8.33: Benefits due to directed beaconing............................................................. 272
Figure 8.34: Increased coverage with HIS & directed antennas, approaching terminal 274
Figure 8.35: Increased coverage only due to directed antennas, departing terminal..... 277
Figure 8.36: Hidden Station Problem with Adaptive Beaconing.................................... 279
LIST OF TABLES

Table 2.1: Summary of UMTS FDD/TDD characteristics ............................................. 13
Table 2.2: Use of S-SCH for Frame Synchronization & Code Group identification ..... 16
Table 2.3: Synchronization/Scrambling Codes for UTRA-FDD/TDD ......................... 19
Table 2.4: Measurement capabilities specified by UTRA TDD/FDD ......................... 25
Table 2.5: Durations in 802.11 standard and amendments ............................................. 34
Table 2.6: Properties of IEEE 802.11 supplements and amendments ......................... 34
Table 2.7: Supported IEs for spectrum management in 802.11h .......................... 51
Table 2.8: RPI levels as defined within 802.11h ..................................................... 55

Table 3.1: WLAN/3G Interworking Scenarios defined within 3GPP [22] ..................... 62
Table 3.2: L2 Trigger generation due to different origins............................................. 96

Table 4.1: Privacy settings and strictness in 3GPP ..................................................... 109
Table 4.2: Exemplary bit/chip durations and impact on position estimation ............... 120
Table 4.3: Accuracy for different precisions in (sub-)urban environments................. 126
Table 4.4: Major GPS Error Sources ......................................................................... 130
Table 4.5: Properties of positioning techniques.......................................................... 138

Table 5.1: Characteristic properties of short-, mid- and long-term data ...................... 149
Table 5.2: 3GPP specifications & reports with respect to Location Services .............. 155
Table 5.3: Selected LCS functions and relation to HIS .............................................. 160
Table 5.4: HIS related to WINNER Logical Node Architecture ................................. 167

Table 6.1: Distance \(d_{\text{max}}\) to be bridged by buffering & VHO to UMTS .......... 184

Table 8.1: Traffic characteristics and QoS parameters for different services .......... 223
Table 8.2: Parameter settings for CM scenario ....................................................... 232
Table 8.3: Characteristic values if CM is introduced ............................................... 234
Table 8.4: RPI histogram thresholds according to 802.11h [74] ............................... 238
Table 8.5: Reference Sensitivity [69] ..................................................................... 238
Table 8.6: Scenario Parameters .............................................................................. 243
Table 8.7: Gain due to initial PHY-Mode recommendation ....................................... 258
Table 8.8: Scenario Service Parameters .................................................................. 260
Table 8.9: Analytical TP loss due to protected beaconing............................................ 268
Table 8.10: Simulated TP loss due to protected beaconing .......................................... 269
Table 8.11: Beneficial application of HIS targeting on maximized WLAN coverage.. 276
[13] ETSI TR 101 683 V1.1.1 (2000-02), Technical Report, Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; System Overview
[14] ETSI TS 101 761-2 V1.1.1 (2000-04), “Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) layer; Part 2: Radio Link Control (RLC) sublayer”
[19] ETSI TR 101 957: Broadband Radio Access Networks (BRAN); HIPERLAN Type2; Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular Systems, V1.1.1 (2001-08).
[21] ETSI DTS/BRAN-0020003-2 v0.c: Broadband Radio Access Networks (BRAN); HIPERLAN Type2; Interworking between HIPERLAN/2 and 3rd Generation Cellular and other Public systems, V0.c (2001-12), equal to TS 101 961  work stopped in 2003
[22] 3GPP TR 22.934 V6.2.0 (2003-09), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking, (Release 6)
[23] 3GPP TS 22.234 V7.2.0 (2005-06), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 7)
[26] 32.2523GPP TS 32.252 V.1.4.0 (2005-05), 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging; (Release 6)
[34] IETF Working Group “Mobility for IPv6 (mip6)”, http://www.ietf.org/html.charters/mip6-charter.html
[40] IST Project WINE GLASS (IST-1999-10669), http://wineglass.tilab.com
Bibliography

less Conference, Mobile and Wireless Systems beyond 3G (EW2004), Barcelona, Spain, February 24-27, 2004


[73] IEEE Std 802.11g-2003, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band”, June 2003


Communication System for Inter System Handover; [FR] Procédé et système de radiocommunication pour transfert inter-système”, AD 27.06.2002, PUB 02.01.2004, Patentschrift EP000001377095A1


[139] ETSI EN 300 328 V1.6.1 (2004-11), “Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2.4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive”


[161] IST-2000-25382-CELLO, project homepage
http://www.telecom.ntua.gr/cello/
[170] IETF Working Group “Geographic Location/Privacy (geopriv)”,
http://www.ietf.org/html.charters/geopriv-charter.html
Technical Specification Group Services and System Aspects; Enhanced
support for User Privacy in location services”, (R5)
[172] 3GPP TS 23.271 V7.0.0 (2005-03), 3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects; Functional
stage 2 description of Location Services (LCS) (R7)
[173] O2online, “Services”,
http://www.o2online.de/o2/kunden/kundencenter/services/
[174] H. Laitinen et al., Deliverable D3, “Cellular Location Technology”, IST-
2000-25382-CELLO, Nov 2001,
http://www.telecom.ece.ntua.gr/cello/documents/CELLO-WP2-VTT-D03-
007-Int.pdf
[175] 3GPP TS 25.305 V7.0.0 (2005-06), 3rd Generation Partnership Project;
Technical Specification Group Radio Access Network; „Stage 2 functional
specification of User Equipment (UE) positioning in UTRAN“, (Release 7)
[176] 3GPP TS 43.059 V7.1.0 (2005-06), 3rd Generation Partnership Project;
Technical Specification Group GSM/EDGE Radio Access Network; “Func-
tional stage 2 description of Location Services (LCS) in GERAN”, (R7)
[177] I. Herwono, J. Sachs, R. Keller, „Integration of Media Point System in
UMTS to provide Session Handover for SIP-based Multimedia Services“, 16th
Annual IEEE International Symposium on Personal Indoor and Mobile
[178] 3GPP TS 02.71 V7.3.0 (2001-03), 3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects; Location Ser-
vices (LCS); Service description, Stage 1 (Release 1998)
[179] 3GPP TS 23.228 V7.4.0 (2006-06), Technical Specification 3rd Genera-
tion Partnership Project; Technical Specification Group Services and Sys-
tem Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 7)
[180] 3GPP2 C.S0022-0 (corresponding to TIA/EIA/IS-801-1), Version 3.0,
„Position Determination Service Standard for Dual Mode Spread Spectrum
Systems“, February 2001
[181] O. Kennemann, “Lokalisierung von Mobilstationen anhand ihrer Funk-
meßdaten”, PhD Thesis, Chair of Communication Networks, RWTH Aach-
http://www.fcc.gov/911
[196] Garmin Ltd., “Global Positioning System (GPS) technology”,
http://www.garmin.com
[197] Gérard Lachapelle, “GPS Challenges!”, Canada Research Chair and
iCORE Chair on Wireless Location, Tampere University of Technology,
21st May 2004
[198] Siemens Press Office Communications, “Siemens brings two new wire-
less modules to market, Radio modules XT75 and XT65”,
http://www.siemens.de/communications, Information Number: COM WM
2006 08.04e, August 16, 2006
GSM positioning technology for high performance Location Based Ser-
vices”, IST Mobile & Wireless Telecommunications Summit 2002, Thessa-
loniki (Greece), 16-19 June 2002.
Project website,
http://europa.eu.int/comm/dgs/energy_transport/galileo/index_en.htm
[201] ETSI TR 101 112 v3.2.0, “Selection Procedure for the Choice of Radio
Transmission Technologies of the Universal Mobile Telecommunication
System (UMTS 30.03)”, Apr. 1998
[202] Federal Ministry of the Interior, Agency and Co-ordination Centre of the
Interministerial Committee for Geoinformation (Interministerielle Aus-
schuss für Geoinformationswesen (IMAGI), “Die Darstellung der Erde in
einer Karte - Projektionen und Koordinatensysteme”,
http://www.imagi.de/de/thema/c_thema_darstellung_erde.html
Project, Department of Geography, University of Colorado at Boulder, Uni-
versity of Texas, December 1999

Non-public references
Contributions from the following diploma- and student project thesis have been
integrated in parts of this work. All theses have been supervised by the author.

Radio Networks”, Student Project Thesis, Chair of Communication
Networks, RWTH Aachen, 2003

Usage of abbreviations is immanent to technical descriptions, specifically in specifications and standards for telecommunications. The present thesis cannot and shall not elude from technical short terms well known to experts. However, for better understanding, each short term is introduced when initially used and listed in the subsequent table for convenient reference.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>ABC</td>
<td>Always Best Connected</td>
</tr>
<tr>
<td>A-GPS</td>
<td>Assisted-GPS</td>
</tr>
<tr>
<td>AIFS</td>
<td>Arbitration Interframe Space</td>
</tr>
<tr>
<td>ALI</td>
<td>Automatic Location Information/Identification</td>
</tr>
<tr>
<td>AoA</td>
<td>Angle of Arrival</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>ARPU</td>
<td>Average Revenue Per User</td>
</tr>
<tr>
<td>AVM</td>
<td>Automatic Vehicle Monitoring</td>
</tr>
<tr>
<td>BER</td>
<td>Bit Error Ratio (Rate)</td>
</tr>
<tr>
<td>BSS</td>
<td>Basic Service Set</td>
</tr>
<tr>
<td>BTS</td>
<td>Base Transceiver Station</td>
</tr>
<tr>
<td>CAPEX</td>
<td>Capital Expenditures</td>
</tr>
<tr>
<td>Cell Id</td>
<td>Cell Identifier</td>
</tr>
<tr>
<td>CCPCH</td>
<td>Common Control Physical Channel (UTRA-TDD/FDD physical channel)</td>
</tr>
<tr>
<td>CCCH</td>
<td>Common Control Channel (UTRA logical channel for signaling during standby)</td>
</tr>
<tr>
<td>CDF</td>
<td>Cumulative Distribution Function</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CGI</td>
<td>Cell Global Identity</td>
</tr>
<tr>
<td>CM</td>
<td>Compressed Mode</td>
</tr>
<tr>
<td>CoG</td>
<td>Centre of Gravity</td>
</tr>
<tr>
<td>ComNets</td>
<td>Chair of Communication Networks</td>
</tr>
<tr>
<td>CoO</td>
<td>Cell of Origin</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Code</td>
</tr>
<tr>
<td>CSD</td>
<td>Circuit Switched Domain</td>
</tr>
<tr>
<td>DCCH</td>
<td>Dedicated Control Channel (UTRA logical channel for signaling within a call)</td>
</tr>
<tr>
<td>DCF</td>
<td>Distributed Coordination Function</td>
</tr>
<tr>
<td>DCM</td>
<td>Database Correlation Method</td>
</tr>
<tr>
<td>DIFS</td>
<td>Distributed Coordination Function Interframe Space</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOTD</td>
<td>Downlink Observed Time Differences</td>
</tr>
<tr>
<td>DSA</td>
<td>Dynamic Spectrum Allocation</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>DTCH</td>
<td>Dedicated Transport Channel (UTRA logical channel for user data)</td>
</tr>
<tr>
<td>E2E</td>
<td>End-to-End (e.g., delay)</td>
</tr>
</tbody>
</table>
| EDCA         | Enhanced Distributed Channel-
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EGNOS</td>
<td>European Geostationary Navigation Overlay Service</td>
</tr>
<tr>
<td>ESA</td>
<td>European Space Agency</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FCFS</td>
<td>First Come First Serve</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame Check Sequence</td>
</tr>
<tr>
<td>FDD</td>
<td>Frequency Division Duplex</td>
</tr>
<tr>
<td>GLONASS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GUID</td>
<td>Globally Unique ID</td>
</tr>
<tr>
<td>HHO</td>
<td>Horizontal HandOver</td>
</tr>
<tr>
<td>HS-DPCCH</td>
<td>High Speed Dedicated Physical Control Channel (UTRA-FDD Physical Channel)</td>
</tr>
<tr>
<td>HS-DSCH</td>
<td>High Speed Downlink Shared Channel (UTRA-TDD/FDD Transport Channel)</td>
</tr>
<tr>
<td>HS-PDSCH</td>
<td>High Speed Physical Downlink Shared Channel (UTRA-TDD/FDD Physical Channel)</td>
</tr>
<tr>
<td>HS-SICH</td>
<td>High Speed Shared Information Channel (UTRA-TDD Physical Channel)</td>
</tr>
<tr>
<td>HS-SCCH</td>
<td>High Speed Shared Control Channel (UTRA-TDD/FDD Physical Channel)</td>
</tr>
<tr>
<td>HO</td>
<td>HandOver</td>
</tr>
<tr>
<td>IBSS</td>
<td>Independent Basic Service Set</td>
</tr>
<tr>
<td>ICT</td>
<td>Information, Communications, Technology</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IPDL</td>
<td>Idle Periods in DownLink</td>
</tr>
<tr>
<td>IR</td>
<td>InfraRed</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>ITU-T</td>
<td>ITU Telecommunication Standardization Sector</td>
</tr>
<tr>
<td>HIPER-LAN/2</td>
<td>High Performance Radio Local Area Network / Type 2</td>
</tr>
<tr>
<td>HMM</td>
<td>Hidden Markov Model</td>
</tr>
<tr>
<td>LA</td>
<td>Link Adaptation</td>
</tr>
<tr>
<td>LAS-CDMA</td>
<td>Large Area Synchronized CDMA</td>
</tr>
<tr>
<td>LCBS</td>
<td>Location Based Services</td>
</tr>
<tr>
<td>LCAF</td>
<td>Location Client Authorization Function</td>
</tr>
<tr>
<td>LCCF</td>
<td>Location Client Control Function</td>
</tr>
<tr>
<td>LCCTF</td>
<td>Location Client Coordinate Transformation Function</td>
</tr>
<tr>
<td>LCF</td>
<td>Location Client Function</td>
</tr>
<tr>
<td>LCI</td>
<td>Location Configuration Information</td>
</tr>
<tr>
<td>LCS</td>
<td>Location Services</td>
</tr>
<tr>
<td>LCZTF</td>
<td>Location Client Zone Transformation Function</td>
</tr>
<tr>
<td>LMS</td>
<td>Location and Monitoring Services</td>
</tr>
<tr>
<td>LMU</td>
<td>Location Measurement Unit</td>
</tr>
<tr>
<td>LSAF</td>
<td>Location Subscriber Authorization Function</td>
</tr>
<tr>
<td>LSBcF</td>
<td>Location System Broadcast Function</td>
</tr>
<tr>
<td>LSBF</td>
<td>Location System Billing Function</td>
</tr>
<tr>
<td>LSCF</td>
<td>Location System Control Function</td>
</tr>
<tr>
<td>LSOF</td>
<td>Location System Operations Function</td>
</tr>
<tr>
<td>LSPF</td>
<td>Location Subscriber Privacy Function</td>
</tr>
<tr>
<td>MCHO</td>
<td>Mobile Controlled HandOver</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MIHO</td>
<td>Mobile Initiated HandOver</td>
</tr>
<tr>
<td>MLME</td>
<td>MAC sublayer management entity</td>
</tr>
<tr>
<td>MM</td>
<td>Mobility Management</td>
</tr>
<tr>
<td>MMC</td>
<td>Mobile Multicast</td>
</tr>
<tr>
<td>MPDU</td>
<td>Medium Access Control (MAC) Protocol Data Unit</td>
</tr>
<tr>
<td>MR</td>
<td>Measurement Report</td>
</tr>
<tr>
<td>MRN</td>
<td>Mobile Radio Network</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Station</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Center</td>
</tr>
<tr>
<td>MSAS</td>
<td>MTSAT-Satellite-Based Augmentation System</td>
</tr>
<tr>
<td>MSDU</td>
<td>MAC Service Data Unit</td>
</tr>
<tr>
<td>MSTH</td>
<td>Medium Sensing Time Histogram</td>
</tr>
<tr>
<td>MT</td>
<td>Mobile Terminal</td>
</tr>
<tr>
<td>MTSAT</td>
<td>Multi Functional Transport Satellite</td>
</tr>
<tr>
<td>NAV</td>
<td>Network Allocation Vector</td>
</tr>
<tr>
<td>NCHO</td>
<td>Network Controlled HandOver</td>
</tr>
<tr>
<td>NIHO</td>
<td>Network Initiated HandOver</td>
</tr>
<tr>
<td>NTRIP</td>
<td>Networked Transport of RTCM via Internet Protocol</td>
</tr>
<tr>
<td>OPEX</td>
<td>Operational Expenditures</td>
</tr>
<tr>
<td>P-CCPCH</td>
<td>Primary Common Control Physical Channel</td>
</tr>
<tr>
<td>PCF</td>
<td>Point Coordination Function</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Density Function</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PER</td>
<td>Packet Error Ratio (Rate)</td>
</tr>
<tr>
<td>PIFS</td>
<td>Point Coordination Function Interframe Space</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>PoA</td>
<td>Point of Access</td>
</tr>
<tr>
<td>PRAF</td>
<td>Positioning Radio Assistance Function</td>
</tr>
<tr>
<td>PRCF</td>
<td>Positioning Radio Coordination/Control Function</td>
</tr>
<tr>
<td>PRRM</td>
<td>Positioning Radio Resource Management</td>
</tr>
<tr>
<td>PSAP</td>
<td>Public Safety Answering Point</td>
</tr>
<tr>
<td>PSD</td>
<td>Packet Switched Domain</td>
</tr>
<tr>
<td>PSMF</td>
<td>Positioning Signal Measurement Function</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RAB</td>
<td>Radio Access Bearer</td>
</tr>
<tr>
<td>RPI</td>
<td>Received Power Indicator</td>
</tr>
<tr>
<td>RSCP</td>
<td>Received Signal Code Power</td>
</tr>
<tr>
<td>RTD</td>
<td>Real Time Differences, Round Trip Delay</td>
</tr>
<tr>
<td>RTCM</td>
<td>Radio Technical Commission for Maritime Services (DPSG correction data)</td>
</tr>
<tr>
<td>SAP</td>
<td>Service Access Point</td>
</tr>
<tr>
<td>SBAS</td>
<td>Satellite-Based Augmentation System</td>
</tr>
<tr>
<td>SDL</td>
<td>Specification and Description Language</td>
</tr>
<tr>
<td>SDR</td>
<td>Software Defined Radio</td>
</tr>
<tr>
<td>SIFS</td>
<td>Short Interframe Space</td>
</tr>
<tr>
<td>SME</td>
<td>Station Management Entity</td>
</tr>
<tr>
<td>SoHo</td>
<td>Small Office/Home Office</td>
</tr>
<tr>
<td>TBTT</td>
<td>Target Beacon Transmission Time</td>
</tr>
<tr>
<td>TDD</td>
<td>Time Division Duplex</td>
</tr>
<tr>
<td>TDOA</td>
<td>Time Difference of Arrival</td>
</tr>
<tr>
<td>TG</td>
<td>Transmission Gap</td>
</tr>
<tr>
<td>TGL</td>
<td>Transmission Gap Length</td>
</tr>
<tr>
<td>TOA</td>
<td>Time of Arrival</td>
</tr>
<tr>
<td>TP</td>
<td>ThroughPut</td>
</tr>
<tr>
<td>TSF</td>
<td>Time Synchronization Function</td>
</tr>
<tr>
<td>TTR</td>
<td>Time To Respond</td>
</tr>
<tr>
<td>TU</td>
<td>Time Unit</td>
</tr>
<tr>
<td></td>
<td>(1 TU = 1024 µs in 802.11)</td>
</tr>
<tr>
<td>TXOP</td>
<td>Transmission Opportunity</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment (UMTS notation for Mobile Terminal)</td>
</tr>
<tr>
<td>UpPTS</td>
<td>Uplink Pilot Time Slot</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>UTM</td>
<td>Universal Transverse Mercator</td>
</tr>
<tr>
<td>VHO</td>
<td>Vertical HandOver</td>
</tr>
<tr>
<td>VoD</td>
<td>Video on Demand</td>
</tr>
<tr>
<td>WAAS</td>
<td>Wide Area Augmentation System</td>
</tr>
<tr>
<td>WCDMA</td>
<td>Wideband Code Division Multiple Access</td>
</tr>
</tbody>
</table>
### INDEX

#### 3
- 3G .......................................................... 58
- 3GPP .................................................... 8, 60
- Location Services .............................. 153
- Vocabulary .......................................... 87
- WLAN interworking ............................ 163

#### 4
- 4G ..................................................... 57, 286

#### 6
- 6th Framework Programme ........... see FP6

#### 8
- 802.11 ..................................................... 30–56
  - Action Frame ........................................ 47
  - backoff ............................................... 32
  - Beacon .............................................. 37
  - channel access ................................... 32
  - Control frame .................................. 45
  - CWmax ............................................... 32
  - CWmin .............................................. 32
  - Data frame ....................................... 45
  - DIFS .................................................. 23, 32
  - legacy .............................................. 31
  - MAC frame formats .......................... 45
  - Management frame ............................ 45
  - NAV ................................................. 33
  - PIFS .................................................. 33
  - Probe frames ................................... 41
  - reference model ................................ 31
  - SIFS .................................................. 33

- Slot Time .............................................. 34
- SSID ................................................... 37
- TBTT ................................................. 38
- TIM .................................................... 37
- working groups .................................. 34
- 802.11h .............................................. 35
- CCA ................................................... 215
- RPI Histogram Report ....................... 215
- 802.11k ............................................. 35, 303
  - Beacon Report .................................. 308
  - Channel Load Report ......................... 307
  - Frame Report .................................... 310
  - Hidden Node Request ......................... 311
  - LCI .................................................. 316
  - Measurement Pause Request ................ 317
  - Measurement Request .......................... 306
  - MSTH Request ................................ 312
  - Noise Histogram Report ....................... 308
  - STA Statistics Report ......................... 314
- 802.11u .................................................. 63
- 802.21 ................................................... 63
- 863 Program ........................................ 69

#### A
- ABC ....................................................... 286
- accuracy ............................................. 134
- adaptive beacon intervals .................. 263
- Advanced Forward Link Trilateration .... 122
- A-GPS ................................................. 126, 129, 132
- Always Best Connected ............ see ABC
- Ambient Networks ......................... 58, 66
- Angle of Arrival ......................... see AoA
- ANWIRE .............................................. 59, 67
- AoA ..................................................... 124
- arc minutes ....................................... 295
- Assisted-GPS ................................. see A-GPS
B

backward handover .................................. 88
Basic Service Set .................................. see BSS
Batch Means ......................................... 208
BCH ..................................................... 16
Beacon .................................................. 37
beacon adaptation strategies .................. 270
Beacon on Demand ................................ 271
beacon protection ................................... 185
Bessel-Ellipsoid .................................... 296
binary reception model .......................... 236
BRAIN ................................................... 67
Break-before-Make see hard handover
Broadcast Channel see BCH
BSS .......................................................... 31

C

CA ........................................................... 31
CAPEX .................................................... 94
Care-of Address ..................................... 91
Carrier Sense Multiple Access see CSMA
CDMA ...................................................... 11
cell border detection .............................. 245
Cell Broadcast Center .............................. 158
CELLO .................................................. 290
cellular handover see L2 handover
Centre of Gravity ................................. 240, 245
Chair of Communication Networks 191, 200
channel models ..................................... 200
channelization codes see spreading codes
chip .......................................................... 11
Clear to Send see CTS
CM ........................................................... 20
Code Division Multiple Access see CDMA
CoG .......................................................... 240
Collision Avoidance see CA
Common Pilot Channel see CPICH
ComNets ................................................ 191
Compressed Mode see CM
Contention Window see CW
correlation .......................................... 175
correlation coefficient ............................ 175
coupling .............................................. 72
    loose ........................................... 60, 62, 69, 145
tight .............................................. 60, 62, 74, 132, 145, 163

covariance ........................................... 175
covariance map ..................................... 243
CPICH ..................................................... 16
CSMA ..................................................... 31
CTS .......................................................... 33
cut-off ............................................... 178
CW ........................................................... 32

D

Database Correlation Method .......... 112, 124
DCF .......................................................... 31
Decision Area ....................................... 240
degrees ................................................. 295
DGPS .................................................... 129, 130
Differential GPS see DGPS
DIFS ..................................................... 23, 32
directed beaconing ................................ 272
Distributed Coordination Function see DCF
Distributed Coordination Function
    Interframe Space see DIFS
DRiVE .................................................... 68

E

E²R ........................................................... 66
E911 .................................................... 104
EDCA ..................................................... 263
EGNOS .................................................. 127
eHIS .................................................... 192, 200
EIRP ...................................................... 277
EMILY ..................................................... 291
End-to-End Reconfigurability see E2R
Enhanced Observed Time Differences see E-OTD
E-OTD ..................................................... 122
error distribution .................................. 173
ETSI ....................................................... 8
ETSI BRAN ........................................... 59, 73
European Commission .......................... 108
European Datum ................................. 297
European Telecommunications Standards
    Institute see ETSI
Index

F

fast handover ........................................... 85
FCC ....................................................... 278
Feeding Clients ..................................... 141
First Come First Serve ......................... 213
flattening ............................................ 294
FLOWS ................................................... 69
Foreign Agent ....................................... 91
forward handover ................................ 88
FP6 .......................................................... 66
FuTURE .................................................. 69

G

GAIA ....................................................... 67
Galileo ............................................127, 133
Gauss-Krueger coordinate system ......... 300
Geodesy ................................................... 293
geodetic datum ...................................... 297
Geoid ..................................................... 293
GGSN .................................................... 156
Global Navigation Satellite System ...... see GNSS
Global Positioning System ............. see GPS
GLONASS .............................................127, 133
GMLC .................................................... 157
GNSS ..................................................... 127
GPS .....................................................126, 127, 297
  Assisted ............................................ 129
  Differential ....................................... 129
  Selective Availability ......................... 129
Greenwich Prime Meridian ................. 295

H

handover

backward ............................................ 88
better cell ........................................... 83
definition ............................................. 81
fast ..................................................... 85
forward ............................................. 88
hard .................................................... 86
hysteresis margins .............................. 82
ideal ................................................... 86
Inter-cell ............................................. 84
inter-system ........................................ 92
Inter-system ..................................... 84
Intra-cell ........................................... 84
L2 (Layer 2) ........................................... 89
L3 (Layer 3) ........................................... 90
Mobile-Controlled .................. see MCHO
Mobile-Initiated ................. see MIHO
network layer ................. see L3 handover
Network-Controlled ........... see NCHO
Network-Initiated ............. see NIHO
ping-pong ....................................... 89, 249
proactive .......................................... 88
radio related ........................................ 89
reason ............................................... 82
Reception quality ................... see GPS
reference sensitivity level .......... 83
seamless ........................................... 85
semi-soft ........................................... 87
service based ............................. 83
service related ............................. 92
smooth ............................................ 85
soft ................................................... 87
softer ............................................. 88
speed based ....................................... 83
Traffic reason ............................ 83
hard handover .............................. 86
HHO ......................................................... 91
Hidden Markov Models ............. 112, 125
hidden station ............................ 279
HIPERLAN/2 ......................................... 59
HIS ................................................... 139–70
  (pro-) active ........................................ 145
  ABC .................................................... 144
  adaptive beaconing ........................... 152
  Data Administration .................... 143
data storage ........................................ 147
  feeding ............................................ 146
  Feeding Clients ............................. 141
  handover triggering ....................... 151
  Information Clients ...................... 141
  LCCTF ............................................ 159
  LCF ................................................... 159
  LCZTF ............................................ 159
  long-term data ............................. 148
  LSOF ................................................ 159
  mid-term data ............................. 148
  overview ....................................... 141
Index

passive mode ..................................... 145
PCF ................................................... 159
PRRM ............................................... 160
PSMF ................................................ 159
reactive mode .................................... 145
self-healing property ......................... 151
Service Control ................................ 143
short-term data .................................. 148
U-LCF .............................................. 159
HMM ............................................... 125, 287
Home Agent............................................. 91
Home Location Register........................ 155
horizontal handover ..................... see HHO
Host mobility .......... see Terminal mobility
Hybrid Information System ............... see HIS
hype cycle ......................................... 105
hysteresis ........................................... 82

I

IBSS ............................................... 32
ideal handover .................................. 86
IEEE ............................................. 30, 63
IEEE 802.11h
   Basic Report .................................. 215
IETF ............................................... 64
IMT-2000 ........................................ 7
Independent Basic Service Set ............. see IBSS
Information Clients.......................... 141
Information Society Technology ....... see IST
Institute of Electrical and Electronics
   Engineers ...................................... see IEEE
Inter-cell handover............................ 84
intermediate hidden station ............. 279
International Telecommunications Union see ITU
Internet Engineering Task Force... see IETF
Inter-system handover ....................... 84
Interworking
   UMTS-WLAN ................................... 60
   WLAN-3GPP .................................. 60
Intra-cell handover ............................. 84
ISO/OSI reference model ..................... 31
IST .................................................. 66
ITU ............................................... 7
ITU-T ............................................. 65

L

L2 handover ...................................... 89
L2 triggers ....................................... 63
L3 handover ...................................... 90
latitude .......................................... 295
LBS .................................................. 103
   application areas ............................. 103
   background .................................... 104
   economics ...................................... 105
   hype cycle ..................................... 105
   privacy ......................................... 107
Limited Relative Error ...................... 208
Link Adaptation ................................ 253
Link Layer Triggers ......................... 63
link state map .................................. 243
LMU .................................................. 158
LOBSTER ........................................... 290
localization ..................................... 102
   accuracy ...................................... 134
   Cell Id .......................................... 116
   Cell of Origin .......... see classification
   integrity ........................................ 135
   pattern recognition .......................... 111
   precision ....................................... 134
   proximity ....................................... 111
   reliability ..................................... 135
   satellite based ................................ 126
   signal strength ............................... 118
   Time Difference of Arrival .............. 119
   Time of Arrival ............................... 119
   triangulation ................................ 110
   trilateration ................................ 110
Location Based Services ................. see LBS
localization error
   error distribution ......................... 173
   evaluation .................................... 174
   modeling ...................................... 172
Location Measurement Unit ............. 119
Location Services ......................... 156
longitude ......................................... 295
loose coupling ................................. 59, 62, 69
LoVEUS ........................................... 291
LRE .................................................. 208
Index

M

Make-before-Break...........see soft handover........242
Manhattan scenario...............242
MCHO.............................................88
Measurement Report.............see MR
Measurements
  802.11...........................................44
  802.11h.........................................49
  802.11k.........................................49
  bilateral....................................114
  multilateral..................................114
  UMTS........................................23
  unilateral.................................114
MIHO...............................................88
MIND................................................67
MIP....................................................91
Mobile IP...........see MIP
Mobile-Controlled HandOver...see MCHO
Mobile-Initiated HandOver ......see MIHO
MobiLife.............................................66
mobiLity
  continuous..................................80
  discrete......................................80
  nomadic.....................................80
  seamless....................................80
  service......................................79
  session.....................................79
  terminal....................................79
  types........................................77
  user.........................................78
MOBIVAS...........................................69
MR
  802.11h......................................56
  density.......................................241
  UMTS.........................................28
MSAS.............................................127

N

NAV..................................................33
NCHO.............................................88
Network Allocation Vector......see NAV
Network-Controlled HandOver ..see NCHO
Network-Initiated HandOver ......see NIHO
Next Generation Networks......see NGN
NGN..................................................65
NIHO...............................................88
Nomadic mobility.....................80

O

Observed Time Difference of Arrival .....see OTDA
OPEX.............................................94
OTDA.............................................122
OverDRIVE....................................68

P

pattern recognition.....................111
P-CCPCH.........................................16, 17
PCF..................................................31
PCF Interframe Space.............see PIFS
Personal mobility ..........see User mobility
PHY-Mode recommendation........256
PIFS.................................................33
ping-pong handover..............89, 249
Point Coordination Function......see PCF
Position Calculation Function ......162
positioning.................................102
  absolute..................................115
  Foreign system based/assisted.....114
  memory-based............................115
  memory-free..............................115
  Network-assisted......................113
  Network-based...........................112
  relative.................................115
  Terminal-assisted.....................113
  Terminal-based.........................113
  precision.................................134
Primary Common Control Physical
  Channel........................................P-CCPCH
Primary Synchronization Channel ....see P-SCH
Primary Synchronization Code ......see PSC
privacy...............................107, 109
  Management Code of Practice.......109
  proactive handover....................88
  propagation model....................237
  propagation models...............200
PSC...............................................15, 17, 19
P-SCH............................................15
Puncturing................................................ 20

R
radio handover .................. see L2 handover
Ready to Send ...................... see RTS
Received Power Indicator........... see RPI
RISE ........................................ 200
roaming ................ see nomadic mobility
rotation ellipsoid.................. 294
RPI........................................... 217
RPI histogram........................ 237
RTS........................................... 33

S
Scanning
802.11....................................... 39
UMTS ........................................ 19
scene analysis ....................... 111
SCH .......................................... 17
SCOUT .................................. 70
scrambling
  code-group ......................... 15
Scrambling................................... 13
SDL ........................................... 192
SDL2SPEETCL ............................. 192
seamless handover .................. 85
Secondary Synchronization Channel... see S-SCH
Secondary Synchronization Code ... see SSC
Selective Availability............... 130
self-healing property ............... 151
self-localization .................... 115
self-soft handover .................. 87
Service mobility...................... 79
Session mobility...................... 79
S-GOOSE ................................ 194, 200
SGSN .................................. 156
Short Interframe Space............ see SIFS
SIFS .................................. 33
SMLC .................................. 158
Smooth handover................... 85
soft handover .......................... 87
Soft handover .......................... 87
Softer handover ..................... 88
Software Defined Radio .............. 58
SPEETCL ................................ 192, 197
  probes ................................. 208
spreading codes ...................... 12
Spreading Factor .................... 13
SSC ....................................... 15, 19
S-SCH .................................... 15
statistical evaluation .............. 208
STRIKE ............................... 70
SUITED ................................ 70
S-WARP ................................ 193
switching point ...................... 12
Synchronization
  802.11 .................................. 37
  UTRA-FDD ............................. 14
  UTRA-TDD ............................ 16
  Synchronization Channel .... see SCH
System integration .................. 59
  access technologies ............... 72
  adaptability and reconfigurability .... 75
  control and management ......... 73
  mobility and handover ............ 74

T
TA ........................................... 123
Target Beacon Transmission Timesee TBTT
TBTT .................................... 38, 185, 264
TDOA ..................................... 119, 121
Terminal mobility ................... 79
TFC ....................................... 20
TG ........................................ 20
TGL ....................................... 20
Third Generation Partnership Project ... see 3GPP
tight coupling ..................... 59, 62
TIM ..................................... 37
Time Difference of Arrival...... see TDOA
Time of Arrival ...................... see ToA
time-of-flight ....................... 110
Timing Advance ........................ see TA
Timing Synchronization Function... see TSF
ToA ..................................... 119, 120
Traffic Indication Messages ... see TIM
Transmission Gap .................... see TG
Transmission Gap Length .......... see TGL
Index

Transport Format Combinations ... see TFC
trigger ...................................................... 95
algorithm-based ...................................... 96
horizontal ............................................. 95
physical-based ...................................... 96
Prioritization ......................................... 99
user preferences ..................................... 98
vertical ................................................ 95
TRUST .................................................... 70
TSF .......................................................... 37
TXOP ..................................................... 185, 264

U
U.C.A.N................................................. 291
UMTS ..................................................... 7–29
active set .............................................. 27, 87
CM ......................................................... 227
detected set .......................................... 27
Frame Duration ..................................... 13
frame structure ...................................... 10
measurement report ............................... 28
measurements ...................................... 23
monitored set ........................................ 27
orthogonality ....................................... 13
orthogonality factor .............................. 229
path loss model ..................................... 229
protocol stack ....................................... 197
rate matching ....................................... 20
Scrambling codes ................................ 13
Symbol Rate ......................................... 13
synchronization .................................... 13
UMTS Radio Access Network ... see UTRAN
Universal Mobile Telecommunications
System .................................................... see UMTS
Universal Transverse Mercator ............. 298
URIS ....................................................... 196, 198
User mobility ....................................... 78
user preferences ................................... 98
UTM ....................................................... 298
UTRA ...................................................... 9
architecture .......................................... 9
Duplex Scheme ................................... 13
FDD ....................................................... 11
TDD ....................................................... 12
UTRAN ................................................... 10

V
Vertical Handover ... see VHO
VHO ....................................................... 84, 91
Business Aspects ................................... 94
Decision Space ...................................... 94
downward ............................................. 92
properties ............................................ 93
Time criticality ..................................... 93
Transparency ........................................ 93
trigger ............................................... 248
upward ................................................. 92
virtual coverage .................................. 183
Visitor Location Register .................... 155

W
WAAS ..................................................... 127
WCDMA ................................................ 10
WGS84 .................................................. 297, 316
Wideband Code Division Multiple Access
.................................................... see WCDMA
WiFi ..................................................... 31
Windowed Link Adaptation ................... 253
WINE GLASS ......................................... 71, 291
WINNER .............................................. 58, 71, 292
Logical Node Architecture ................. 165
Wireless Local Area Network ... see WLAN
Wireless World Initiative ................. see WWI
Wireless World Research Forum ... see WWRF
WLAN .................................................. 30
World Geodetic System ...................... 297
WWI ....................................................... 66
WWRF ................................................... 65
ACKNOWLEDGEMENT

This thesis is the outcome of my exciting time as research assistant at the Chair of Communication Networks (ComNets), RWTH Aachen University. During this time, I was given the particular chance to graduate in many disciplines simultaneously: Being part of and contributing to leading scientific research, managing international projects and cultivating social skills are experiences that probably no other occupation offers at such an intensity while nice atmosphere.

I am deeply grateful to Prof. Dr.-Ing. Bernhard Walke for the extraordinary opportunity having been part of ComNets. Besides serving as supervisor for this thesis, he was a great mentor during all these years. His impressive reservoir of new ideas and visions is only one out of many attributes, which is worth mentioning.

I further thank Prof. Dr. rer. nat. habil. Carmelita Görg, Chair of Communication Networks, University of Bremen, for her disposition to serve as second examiner. Her valuable feedback is highly appreciated.

There are many other colleagues of mine that I would like to mention here and say thank you: First, Dr. Stefan Mangold who served as the supervisor of my diploma thesis and paved my way into the scientific world resulting in more than forty scientific publications and patents so far. Right from the very beginning, Dr. Ingo Forkel was my ComNets companion. We became friends and without being immodest, I guess we established some kind of new culture at the chair and made things move. During my first two years at ComNets, I worked alongside with Dr. Matthias Lott sharing the same office. Our successful cooperation did not end with his change over to industries. In fact, there were many other joint projects, papers and patents to come and our exhausting professional life was only beaten by our even more exhausting sports battles. For the last three years, I shared my office with my colleague and friend Ralf Pabst and I will miss our highly intellectual Simpsons discussions. I guess I will be in his debt for another decade for all the patience he needed to exercise, particularly with respect to a particular piece of furniture that I used to accommodate in our office.

No thesis can be written without the particular support from students and diploma workers, all of which shall be included in this acknowledgement. Special thanks goes to Marc Schinnenburg, Stephan Goebbels and Daniel Bültmann that also became colleagues of
mine at ComNets. In contributing to my projects, they have a share in the successful realization of this thesis. Particularly Daniel was a big aid and I really appreciate his support. Furthermore, I am happy that he will continue my scientific work on location-based networking.

Besides the so far mentioned people, some other helping hands shall not be forgotten: Daniel Schultz, Guido R. Hiertz, Tim Irnich, Dr. Lars Berlemann and Dr. Michael Pilling for their review activities, Heinz Rochhausen for his perfect back office support during all these years and Karin von Czapiewski for her engagement as our former ComNets- and current faculty secretary.

All other (former) ComNets colleagues that cannot be mentioned here by name shall be said thanks as well, for their cooperative work and the nice time including many social events and lots of fun.

Finally, I would like to single out my family for keeping me grounded during all this years. A special thanks goes to my parents that made all this possible by providing me a solid financial basis and genial base camp. During my entire studies, I could concentrate on the essentials, which they can take credit for. Also thanks to my parents-in-law for continuing giving me the same genial base-camp in ‘Oche’.

My particular thanks goes to my beloved wife Moni for her continuous support, love, lots of understanding and some deprivations, too. This thesis somehow is hers as well. Finally many thanks to the sweetest baby on world, Lilli, just for being there and smiling at me.

Pfungstadt, December 2006

Matthias Siebert
<table>
<thead>
<tr>
<th>Date Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>04. July 1971</td>
<td>Born in Wettingen/Switzerland</td>
</tr>
<tr>
<td>08/1978 – 06/1982</td>
<td>Gemeinschaftsgrundschule Stakerseite</td>
</tr>
<tr>
<td></td>
<td>Kaarst</td>
</tr>
<tr>
<td></td>
<td>Kaarst</td>
</tr>
<tr>
<td></td>
<td>Wuppertal/Cologne</td>
</tr>
<tr>
<td>07/1992 – 09/1992</td>
<td>Internship at Schiess AG</td>
</tr>
<tr>
<td></td>
<td>Düsseldorf</td>
</tr>
<tr>
<td></td>
<td>RWTH Aachen University</td>
</tr>
<tr>
<td>09/1997 – 03/1998</td>
<td>Semester abroad with Student Project Thesis</td>
</tr>
<tr>
<td></td>
<td>Centre for Vision Speech &amp; Signal Processing, University of Surrey, U.K.</td>
</tr>
<tr>
<td>03/1994 – 04/1994</td>
<td>Internship at Siemens AG</td>
</tr>
<tr>
<td></td>
<td>Düsseldorf</td>
</tr>
<tr>
<td>02/1995 – 04/1995</td>
<td>Internship at Unitronic GmbH</td>
</tr>
<tr>
<td></td>
<td>Düsseldorf</td>
</tr>
<tr>
<td>04/1998 – 05/1998</td>
<td>Internship at STAWAG AG</td>
</tr>
<tr>
<td></td>
<td>Aachen</td>
</tr>
<tr>
<td>06/1999 – 11/2005</td>
<td>Research Assistant at the Chair of Communication Networks</td>
</tr>
<tr>
<td></td>
<td>RWTH Aachen University</td>
</tr>
<tr>
<td>Since 12/2005</td>
<td>Professional Research and Development Engineer</td>
</tr>
<tr>
<td></td>
<td>T-Systems Enterprise Services GmbH, Darmstadt</td>
</tr>
</tbody>
</table>