Mobile-Controlled Handover in Wireless LANs

Diplomarbeit
der Philosophisch-naturwissenschaftlichen Fakultät
der Universität Bern

vorgelegt von:
Attila Weyland

2001

Leiter der Arbeit:
Prof. Dr. Torsten Braun

Forschungsgruppe Rechnernetze und Verteilte Systeme (RVS)
Institut für Informatik und angewandte Mathematik

Contents

Preface

Wireless LAN technology with Mobile IP as extension to the Internet Protocol is currently a common base in mobility works.

Mobile IP acts as routing protocol on the network layer and does therefore not specify any control mechanisms for the wireless LAN hardware.

With the increasing importance of intelligent network management solutions (i.e. Quality of Service Accounting and Provisioning), a better reference to and inclusion of the wireless LAN hardware is required to allow seamless handovers and thus deliver reliable mobile application services.

By evaluating the state and controlling the behavior of the wireless LAN hardware, future movements of mobile nodes to other access points can be identified and therefore necessary actions can be taken in due time.

While hardware is always manufacturer specific, it also complies to standards. In this particular case it was important to choose values and methods defined in the IEEE 802.11 standard.

The approach presented in this diploma thesis uses control mechanisms based on the Signal-to-Noise ratio of the wireless links to available access points. Crucial changes are advertised to concerned applications, which in turn can make all necessary preparations for a fast handovers.

Chapter 1

General Introduction

This chapter explains the current situation in the mobile sector, introduces some proposed solutions and presents the approach taken in this thesis.

1.1 Current situation

While the wireless LAN technology spreads more widely, available Mobile IP implementations do not yet handle handovers satisfactorily.

The wireless LAN technology has been in use for a long time now (over 10 years) and mature, standardized products are available. Due to the implementation in hardware, the link layer handover process concludes very quickly. However, most manufacturers do not implement enough control over their products, making it difficult to adjust or improve the wireless LAN hardware's behavior.

The design of Mobile IPv4 is restricted by the abilities of IPv4 and leaves a lot of room for improvements. Especially the reduction of the handover latency is a topic widely discussed.

And although IPv6 provides better prerequisite (in terms of flexibility and extensibility) for the implementation of a mobility support protocol, Mobile IPv6 still has some flaws.

One of the major concerns is, that while the wireless LAN technology and Mobile IP operate at different layers (the first at the physical and the link layer, the latter at the network layer), there is no definition for the inter layer communication between link and network layer. In practice, this is reflected in the Mobile IP implementations just following the behavior of the wireless LAN hardware. Of course, this leads to delays or unwanted and unpredictable results.

But especially for applications relying on QoS, the well timed transfer of network management information (i.e. flow descriptors) to the new point of

attachment is very important. This can only be guaranteed, if control over the link layer handover process is provided to these applications.

By the time, specific terms for handover improvements have become common. A *Fast Handover* primarily aims to minimize delay of the handover process, a *Smooth Handover* primarily aims to minimize packet loss. A *Seamless Handover* is both, fast and smooth.

1.2 Proposed solutions

Only few of the proposed solutions implement inter layer communication, most of them define rather complex extensions to the mobility support in IPv4 and IPv6 (see Section 5.3 for a detailed description).

The paper "Optimized Smooth Handoffs" [26] addresses three issues in Mobile IPv4: triangle routing, out-of-date location information and frequent handovers. The solution proposed implements route optimization, a buffering mechanism and hierarchical FA management.

In "Low Latency Handoffs" [7], methods to minimize the latency caused by the Mobile IPv4 registration process, are proposed. The design includes pre- and post-registration mechanisms as well as link layer triggers.

With "QoS-Aware handover for Mobile IP" [4] handovers are performed on the base of available resources. The maintenance of the old reservation until the successful completion of the new one aim to provide a constant QoS level.

The Internet Draft "Fast Handovers for Mobile IPv6" [6] attempts to reduce latency of the Mobile IPv6 registration process. Several new messages have been defined as well as the usage of link layer triggers.

Unfortunately, when used in a proposal, link layer triggers are not specified in detail. Also, most solutions add additional administrative overhead or put short high peak load on the wireless network, which still is short of bandwidth.

1.3 Another approach

The need to rely on link layer information to allow certain means of synchronization between the different layers involved in the handover process is understood.

The most obvious parameters that influence the wireless LAN hardware's behavior are indicators of the signal quality. These quality parameters are usually provided by the driver of the wireless LAN hardware and can be gathered easily.

This leads to the main idea to continuously monitor the signal quality and, upon exceeding or falling below certain thresholds, alert concerned applications.

The implementation requires access to the wireless LAN hardware, a specification of the thresholds (Chapter 4) as well as a communication interface to other programs (Chapter 6).

With these abilities a mobile node is in control over the handover process and can perform fast handovers.

Chapter 2

Wireless LANs

Over the years wireless LANs have become more and more popular, thus making standardization necessary and important. This chapter explains the available technologies, gives a brief historical outline of the standardization process and describes todays dominant standard, IEEE 802.11, and one commercial implementation, WaveLAN, in detail.

2.1 Wireless LAN technology

Different technologies exist to transmit information through the air using electromagnetic waves. A broad classification of these technologies results in two types of LANs: radio and infrared (IR). While radio LANs use narrowband or spread spectrum transmission, infrared LANs use diffuse or directed. The following sections describe the several types of transmission.

2.1.1 Narrowband transmission

A narrowband radio system uses a specific frequency to transmit the information whereat the bandwidth of that channel is kept as narrow as possible (see Figures 2.1 and 2.2).

Its narrowband attribute makes it easy to jam the signal or spy on the transmitted information. Each frequency in use must be licensed by the appropriate international regulatory bodies.

2.1.2 Spread spectrum transmission

First developed by the military in need of a reliable and secure communication system, spread spectrum technology is finding use in the commercial sector.

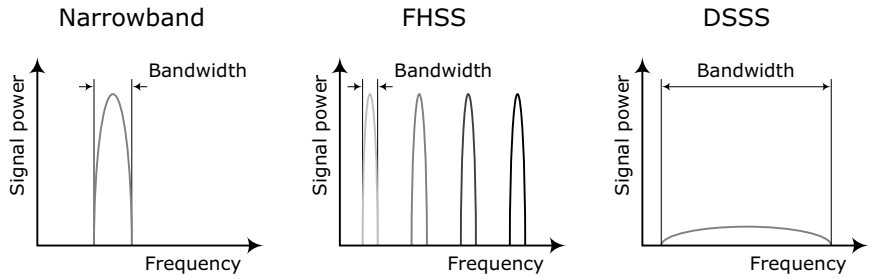

Figure 2.1: Transmitted energy distribution over frequency spectrum

The use of a much wider bandwidth, than actually required, to transmit the information, assures that disturbances (e.g. interference) affect only a small part of the transmission. Different coding schemes, which are independent of the message, provide the necessary security. Three frequency bands have been made available for license free use under conditions determined by the responsible international regulatory bodies (see Section 2.2).

Two spread spectrum techniques exist: frequency-hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS).

2.1.2.1 Frequency-hopping spread spectrum

After emitting a short burst on one frequency channel, FHSS changes to another channel and repeats this action in a short period of time following a predefined pattern (see Figure 2.1) known to both transmitter and receiver. By means of synchronization they always keep an equal position in the pattern.

To an unintended receiver, FHSS appears to be short-duration impulse noise (see Figure 2.2).

2.1.2.2 Direct-sequence spread spectrum

By spreading the energy of the signal over a large bandwidth (see Figure 2.1), DSSS reduces the energy per unit frequency and thus significantly lowers the interference produced compared to narrowband systems. Hence multiple DSSS signals can share the same frequency band.

DSSS combines the digital bitstream source with a higher speed binary code. Thereby each source bit is mapped into a bit pattern, called chipping code, known only to the transmitter and the intended receiver. The longer the chipping code, the greater the probability to recover the original data in case transmission errors occur.

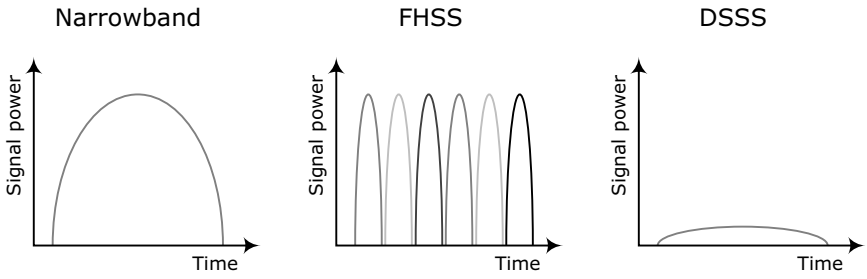

Figure 2.2: Transmitted energy distribution over time

To an unintended receiver, DSSS signals appear as low-power wideband noise (see Figure 2.2) and are rejected by most narrowband receivers.

2.1.3 Infrared transmission

IR systems operate at very high frequencies. IR light is very close to visible light in the electromagnetic spectrum (i.e. near in wavelength) and therefore has similar physical properties. It can not penetrate opaque objects and passing through windows will attenuate it significantly. Thus IR systems are limited to operate within a single room.

IR links are based on on-off pulse modulation, similar to an optical fiber network. Information is carried by the intensity of the light wave. This stands in contrast to the methods described above (see Sections 2.1.1 and 2.1.2) where the frequency or the phase is used.

However, since no license is required to operate at these high frequencies and components are small in size and consume little power, IR transmission is still a common choice.

Two infrared transmission techniques exist: directed infrared and diffuse infrared (DFIR).

2.1.3.1 Directed infrared

Since directed IR systems require line-of-sight to operate, transmitter and receiver have to be pointed toward each other, thus not allowing great mobility. Long range, high performance infrared LANs are implemented as fixed networks.

2.1.3.2 Diffuse infrared

DFIR systems use reflected infrared energy to transmit information. Transmitter and receiver are often pointed at the ceiling, which acts as diffuse

reflector. Although line-of-sight is not required, cells are limited to single rooms. Hence mobility is restricted too.

2.2 Wireless LAN standards history

Two major standardization activities for wireless LANs have taken place in the past decade.

2.2.1 The IEEE 802.11 standard series

In 1985, The Federal Communications Commission (FCC) designated the frequency ranges at 902-928 MHz, 2400-2483.5 MHz and 5725-5850 MHz as license-free for spread-spectrum devices in the United States.

These three bands have been allocated for industrial, scientific and medical use and are therefore called the ISM bands. In mid-1990, the Institute of Electrical and Electronics Engineers (IEEE) formed a committee (the 802.11 working group) to define a manufacturer-independent standard in these bands. It [14] has been ratified in July 1997 and provides 1 and 2 Mbps data rates.

After Lucent Technologies announced that new modulation techniques allow much higher data rates, new standardization efforts started. This work concluded in the IEEE 802.11b standard extension, completed in 1999 and realizing up to 11 Mbps, though bound to the DSSS transmission method (see Section 2.1.2.2 for a more detailed explanation). In the same year the IEEE 802.11a standard has been ratified. It defines a high-speed transmission in the 5 GHz band, supporting data rates up to 54 Mbps.

Approved in late 2001, the IEEE 802.11g standard is an advancement to the IEEE 802.11b standard. Although the first standard operates in the same spectrum (2.4 GHz band) as the latter, their underlying techniques differ from each other, making downward compatibility expensive. By the use of a different access method (Orthogonal Frequency Division Multiplexing, OFDM) the 802.11g standard doubles the maximum data rate to 22 Mbps.

The IEEE 802.11(b) standard has been implemented widely and a broad range of products are available, partly ruled out by 802.11b compliant products. Moreover some vendors start to offer 802.11a based chip sets, taking advantage of the high data rates and the availability of frequencies on the not yet crowded 5 GHz band.

2.2.2 The HIPERLAN standard series

The second endeavor to develop a standard for wireless networks took place in Europe. In mid-1991, the ETSI (European Telecommunication Standards

Institute) appointed a technical subgroup to this task.

Two years later, the Conférence européenne des administrations des postes et des télécommunications (CEPT) allocated the spectrum to be used (5150-5250 MHz). The final approval of the High PErformance Radio Local Area Network Type 1 (HIPERLAN/1) [8] standard occurred in mid-1996. With a data rate of 20 Mbps it has been targeted at broadband wireless communications.

However, during its completion it became apparent that the standard did not satisfactorily cater for connections to IP and ATM and thus new standards called HIPERLAN 2, 3 and 4 have been developed. Despite these efforts HIPERLAN technology is not widely used until now.

2.2.3 Additional standardization work

While the above standards where developed to provide a common interface to already existing hardware, new standards currently emerging for the home sector don't have this burden.

New fields of application in this sector (e.g. wearable devices) require low-cost and low-power-consumption components. To meet those demands the newly founded 802.15 working group has been charged with the development of a new standard covering the requirements of wireless Personal Area Networks (PANs). The Bluetooth standard, also belonging to this new category and being widely supported, deserves to be mentioned too.

2.3 The IEEE 802.11 wireless LAN standard

Being a standard for a different network field compared to the longstanding and well-known wired networks (e.g. IEEE 802.3 and 802.4), further explanation of its terminology and conceptualized network structure is necessary.

Like every IEEE 802 standards, this wireless standard introduces new sublayers (see Figure 2.3) to the existing layers from the ISO/OSI Basic Reference Model [15].

It includes three different physical layers (PHY), each one describing the implementation of one of the following transmission methods: FHSS, DSSS and DFIR (see Sections 2.1.2.1, 2.1.2.2 and 2.1.3.2).

Additionally the media access control (MAC) is specified. The MAC layer includes some functionality from the logical link control to hide specific wireless behavior from higher layers.

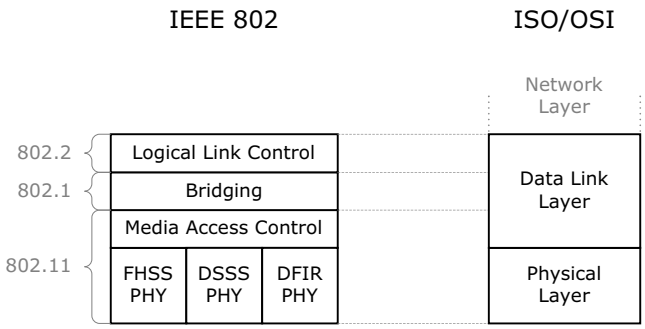

Figure 2.3: IEEE 802 layers vs. ISO/OSI Basic Reference Model

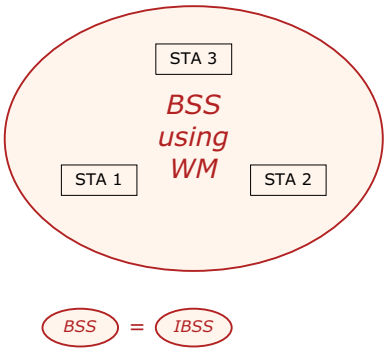

Figure 2.4: Independent basic service set network

2.3.1 Network terminology and topologies

The standard introduces new terms to describe typical wireless components.

The mobile and portable devices are referred to as *stations*. The *basic service set* (BSS) represents the coverage area in which member stations can remain in communication over the *wireless medium*. The *basic service set identifier* (BSSID) is equivalent to a network name for the BSS. Normally it corresponds to the MAC address of the wireless LAN card.

To allow communication between different BSSs the *distribution system* (DS) provides the necessary interconnection. The key component of the DS is the *access point* (AP). Apart from possessing all the functionality of a station, it also acts as a bridge between the wireless medium and the *distribution system medium* (DSM).

Two main LAN types have been described by the standard. The first one is called the *independent basic service set* (IBSS) network. It consists of two or more stations which communicate directly only over the wireless medium (see Figure 2.4). This network type is often referred to as *ad hoc network*

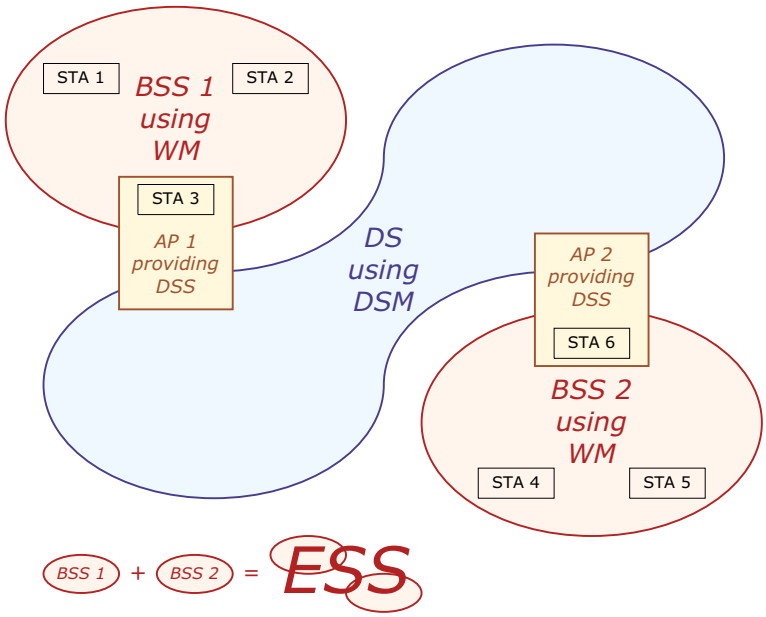

Figure 2.5: Extended service set network

because it requires no pre-planning to form such a network and therefore can be instantly set up almost everywhere.

The second type combines multiple BSSs to achieve a larger coverage. The connection between different BSSs is provided by APs over a DSM. The DSM can be either wireless or wired. Such an interconnection of BSSs is called the *extended service set* (ESS) network (see Figure 2.5). The *extended service set identifier* (ESSID) enables the unique identification of the ESS. To allow stations to roam between different BSSs, a common ESSID has to be defined.

The IEEE 802.11 standard does not specify the details of DS implementations. Instead it specifies *services*, that DS implementations have to provide.

2.3.2 Services overview

Two categories of IEEE 802.11 services exist: the *station service* (SS) and the *distribution system service* (DSS). They are both used by the IEEE 802.11 MAC sublayer (see Section 2.3.3).

This sublayer uses three type of messages: *data*, *management* and *control*. MAC management messages support the different services, while MAC control messages support the delivery of management and data messages.

The following two sections describe those services necessary for the under-

standing of the link layer handover process. A complete coverage can be found in the standard [14] itself.

2.3.2.1 Station services

In contrast to wired LANs, physical security is not feasible for wireless LANs due to the open nature of the wireless medium.

In order to control LAN access the *Authentication* process has been defined. Using this service a station establishes its identity to other stations (including APs) with which it wants to communicate. Since authentication is required for association, invoking the *Deauthentication* service causes a station to be disassociated, apart from terminating its authentication.

The IEEE 802.11 standard specifies two mechanisms for authentication:

- Open System
  An authentication request will always result in a positive authentication response
- Shared Key
  It uses the wired equivalent privacy (WEP) encryption scheme, where identity is demonstrated by knowledge of a shared key.

Note: The WEP scheme is based on the RC4 cipher, which has been proved to be dangerously vulnerable [9]. A passive network attack using weaknesses in the RC4 key scheduling algorithm allows the retrieval of the 40-bit network key in less than 15 minutes. To make things worse, the attack system scales linearly, rendering the key length as security factor useless.

2.3.2.2 Distribution system services

The distribution system service needs to know which AP in the DS gives access to the receiver (i.e. a station) of a (data) message. The concept of *Association* provides this information to the DSS.

To send a data message via an AP a station must first associate with this AP. At any time a station can be associated with only one AP. This unique mapping of stations to APs ensures the precise determination of a station's location (i.e. the AP it is currently served by, associated with). Association corresponds to connecting a station to the LAN.

The *Reassociation* service meets the mobility requirements by allowing transitions between different BSSs. It permits to move the current association from one AP to another, thus keeping the mapping between AP and station

in the DS up-to-date. Reassociation also enables the change of association attributes, while preserving this association with the AP. Reassociation updates an existing connection.

With the *Disassociation* service an existing association is terminated.

2.3.3 MAC sublayer operations

This section describes additional functionality provided by IEEE 802.11 MAC sublayer. Furthermore the implementation of the services introduced in Section 2.3.2.2 is explained.

2.3.3.1 Scanning

A scan monitors a chosen channel for available APs. The following two methods exist:

Passive scanning implies that the station listens to the beacon messages transmitted from the APs on the selected channel.

When using *active scanning*, the station sends a probe request on a channel and waits for a probe response from eventual available APs.

2.3.3.2 Association and reassociation

The association procedure requires the following steps to be taken. First, the station sends a association request frame to an AP. If the station is authenticated, the AP replies with a association response frame. In return the station acknowledge the successful reception of the response. Now the AP notifies the DS about the changes.

Similarly, reassociation follows the same procedure, but uses its own (reassociation) request and response frames. Also, the old AP will be notified about changes via the DS by the new AP.

2.4 WaveLAN operation

WaveLAN is a commercial wireless LAN implementation from Lucent Technologies conforming to the IEEE 802.11 standard.

The following description of the link layer handover process is based on the WaveLAN implementation (see [18]).

The wireless LAN card permanently monitors the signal quality of its current link to the AP. These values are compared reiteratively with predefined thresholds and lead to appropriate actions.

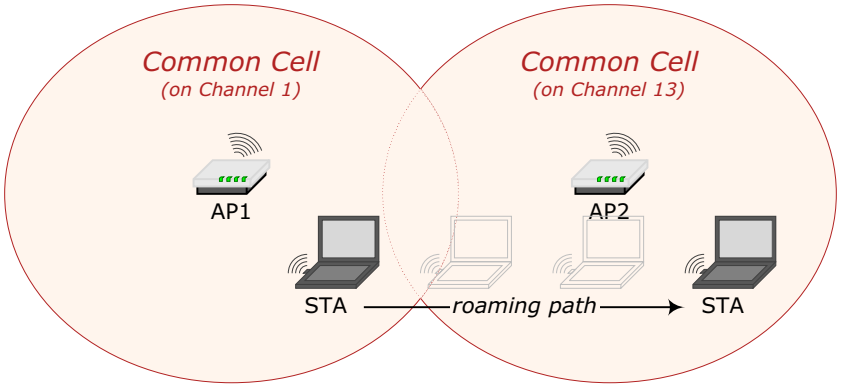

Figure 2.6: Roaming between two wireless cells

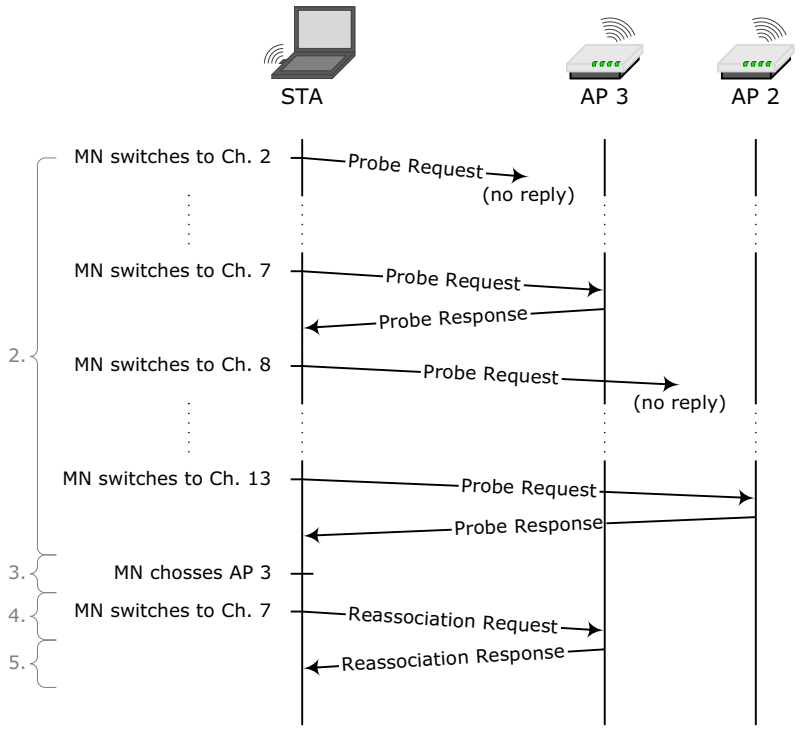

Figure 2.7: Link layer handover message-time diagram using active scanning

2.4.1 Link layer handover procedure

When a station moves to the border of the coverage area (so-called wireless cell) of its current AP into the coverage area of another AP (see Figure 2.6), the signal quality of the current link drops and a process called *Handover* is invoked. It guarantees the seamless transition between different wireless cells up to the link layer.

These steps describe the link layer handover procedure shown in Figure 2.7 in detail:

1. A station decides (see Section 2.4.3) that the signal quality to the current AP is poor.
2. It starts to look for other APs with the same ESSID using a sweep.

   (A sweep characterizes a series of scans (see Section 2.3.3.1) on different channels. These are maintained by the station in a channel-list).
3. The station then selects the best AP found by evaluating the signal quality.
4. It sends a reassociation request to the selected AP. The AP determines if access can be granted (see Section 2.3.2.1).
5. If the station is allowed to access the AP, the AP sends a reassociation response.

2.4.2 Measurement categories

When monitoring the signal quality, the *Signal-to-Noise Ratio* (SNR) is of substantial interest. It is based on the signal level and the noise level. The signal level is obtained from the beacon messages sent by all APs at a rate of ten messages per second. Information about the noise level is taken from the data traffic the station is engaged in.

2.4.3 Decision points

A well timed identification of the station's movements is achieved by introducing several decision points (thresholds) based on the SNR values (see Section 2.4.2).

Table 2.1 lists the thresholds depending on the density of installed APs. The AP density value specifies the distance between APs in the wireless network. These values are taken from Lucent's Technical Bulletin 023/B [19].

Threshold	AP Density		
	Low	Medium	High
Carrier Detect [dBm]	-95	-90	-85
Defer [dBm]	-95	-85	-75
Cell Search [dB]	10	23	30
Out of Range [dB]	2	7	12
Delta SNR [dB]	6	7	8

Table 2.1: WaveLAN/IEEE thresholds

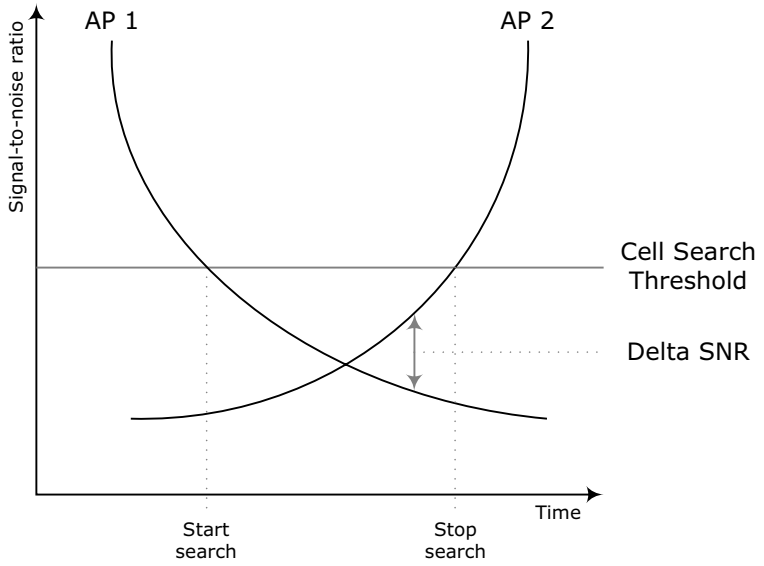

Figure 2.8: Link layer handover SNR-time diagram

Carrier Detect threshold: A signal level value in dBm representing a lower limit. A station will only accept received signals that exceed the Carrier Detect threshold.

Defer threshold: A signal level value in dBm marking an upper bound. A station will delay its own signal to be transmitted until the incoming signal falls below the Defer threshold, thereby not being recognized as a modem signal anymore.

Cell Search threshold: A SNR value in dB used as lower bound. A station will start to look for another AP as soon as the SNR falls below the Cell Search threshold.

Out of Range threshold: A SNR value in dB describing a lower limit. A station will be unable to receive a signal properly if the signal's SNR falls below the Out of Range threshold.

Delta SNR: A SNR value in dB representing a minimal distance. A station will only change to another AP if the difference of both, the old and the new AP's SNRs exceed the Delta SNR.

Figure 2.8 depicts the thresholds impact in the scenario seen in Figure 2.6.

Over time the station shifts from the Wireless Cell 1 to the Wireless Cell 2. Thereby it removes from the first AP and thus the SNR decreases more and more. Soon the SNR falls below the *Cell Search* threshold, triggering the scanning functions of the wireless LAN card. When it recognizes the second AP, the wireless LAN card does not connect instantly to the new AP. Instead it waits for the difference between the SNR from AP1 and AP2 to exceed the *Delta SNR*. After having changed to AP2, the wireless LAN card stays in the search state until the SNR passes the Cell Search threshold again.

If the station moves to an area without any AP coverage, the SNR falls below the *Out of Range* threshold, causing more intense scans. Another reason for not finding any APs might be an overloaded network.

Chapter 3

Mobile IP

The wireless LANs discussed in Chapter 2 allow seamless transitions up to the link layer. However, when the mobile device covers a larger distance, it will most probably cross router boundaries (i.e. move to a new IP domain). By doing so, the mobile device invalidates its IP address, so the network layer protocols too, need to accommodate the requirements of mobility.

3.1 Mobile IPv4 overview

The Mobility Support in IPv4 is a proposed standard, which has been designed by a working group within the Internet Engineering Task Force (IETF) to support node mobility. It enables mobile devices to stay connected to the Internet regardless to any (geographical and administrative) changes to their location. Mobile IPv4 accomplishes this by setting up and maintaining routing tables in the appropriate places. Therefore, it can be seen as a specialized routing protocol.

Operating at the network layer, Mobile IPv4 is completely independent of the media over which it runs. It allows a mobile device to move between different media types while retaining its connectivity. This ability is called *heterogeneous mobility*.

3.2 Mobile IPv4 design details

The following sections will provide selected information about Mobile IP, which represent prerequisites for later chapters.

A comprehensive description can be found in the standards documents, which include several Request for Comments (RFCs), among them RFC 2002 [23] (describing the protocol itself), RFC 2003, RFC 2004 and RFC

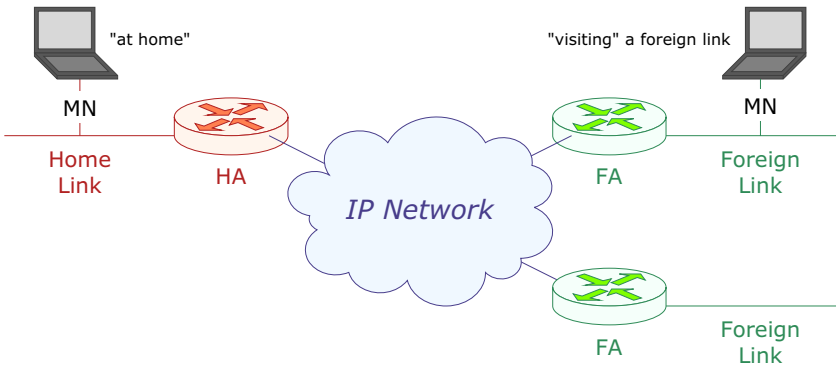

Figure 3.1: Mobile IPv4 entities and their relationship

1701 [22, 24, 13]. For extensive background knowledge [27] represents a reliable source.

3.2.1 Entities

Based on Figure 3.1 the basic functional entities of Mobile IPv4 will be explained.

A *link* represents a medium over which a *node* (i.e. a host or a router) can communicate at the link layer level.

The mobile device is referred to as *mobile node* (MN). During a change of its point of attachment to a new link, the MN maintains any ongoing communication and keeps using its permanent IP *home address*. Other correspondent hosts will use this address when sending packets to the MN, regardless of its current location.

To ensure it is always trackable, the MN notifies the *home agent* (HA) about all location changes by sending the assigned *care-of address* (COA). When the MN is away from home, the HA acts as router and forwards encapsulated packets addressed to the MN by using the COA, which can be seen as the exit-point of the tunnel residing at the FA or the MN's interface.

The *foreign agent* (FA) is the default router for packets generated by the visiting MN. Furthermore it can provide the COA for the MN (the so-called *foreign agent care-of address*, FA COA) and de-tunnel packets for the MN from the HA. The FA COA can be shared by many MNs simultaneously. The FA also assists the MN when informing the HA about the current COA. Another type of care-of address exists: the *collocated care-of address*. It is assigned to the MN's interface itself and used in situations where no FA is available on the current link. The collocated COA can be used by only one MN.

The term *mobility agent* refers to an agent which supports mobility. It can be either a HA or a FA.

A node which is in communication with the MN is called *correspondent node* (CN). It may be either mobile or stationary.

3.2.2 Supported services

To support the Mobile IPv4 operation the standard describes several services, which must be provided for proper functioning.

Agent Discovery: The mobility agents broadcast their availability on each link to where they can provide service. These messages are called *agent advertisements*. A MN can also advertise its arrival to a new link with an agent solicitation message to which available mobility agents would reply.

Registration: When the MN is visiting foreign links, it registers its COA with its HA, so that the HA knows where to forward packets destined to the MN. Depending on the network configuration, the registration can occur directly with the HA or indirectly via the FA.

Encapsulation: An IP datagram is enclosed within another IP header, thus forming a new IP packet. The IP destination address of the wrapping header is set to COA of the MN. The original IP datagram remains untouched throughout the enclosing process.

Decapsulation: The outermost IP header is removed from the incoming packet and the enclosed datagram is delivered to the proper destination. Decapsulation is the reverse process of encapsulation.

3.2.3 Overall process

Figure 3.2 illustrates the Mobile IPv4 operations layout now described thoroughly:

1. The mobility agents broadcast periodically agent advertisements on their respective link.

2. MNs examine received agent advertisements and decide whether they are connected to their home or a foreign link.

   (MNs connected to their home link just act like stationary nodes and make no more use of Mobile IPv4 functionality.)

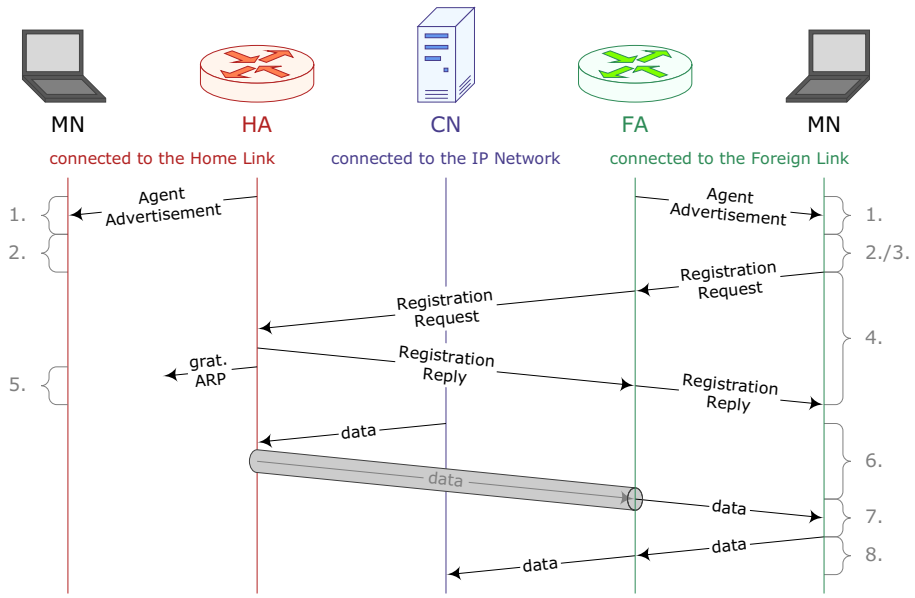

Figure 3.2: Mobile IPv4 operation Time-Message-Diagram

3. The MNs connected to a foreign link obtain a FA COA from the agent advertisement or a collocated COA from other protocols (e.g. DHCP).

4. Now the MN registers its COA with its HA.

5. The HA or other routers on the home link send gratuitous ARP messages with the network prefix equal to the MN's home address, thereby attracting packets destined for the MN.

6. Upon reception of such packets from a CN the HA tunnels them to the COA of the MN.

7. At the COA (either the FA or a MN interface) the original packet is extracted from the tunnel and then delivered to the MN.

8. Any packets sent by the visiting MN are routed by the FA directly to their destination.

3.3 Mobile IPv4 implementations

Today a considerable number of Mobile IPv4 implementations exists for Linux and UNIX systems. By now the most commonly used is Dynamics [11] from the Helsinki University of Technology.

Dynamics has also been used during the realization of the work described herein. For a detailed explanation of the Dynamics software and an overview of more available Mobile IPv4 solutions see [30].

3.4 Mobile IPv6 summary

The specification of a standard covering mobility support in IPv6 is still in progress and therefore only an Internet Draft [16] is available by now.

3.4.1 Comparison with Mobile IPv4

The lack of the IPv4 limitations in IPv6 [5] influences the definition of Mobile IPv6.

In Mobile IPv4, the FA eliminates the need to assign a unique collocated COA to each MN, thus saving a lot of addresses. Since IPv6 has an enormous address space and allows simple autoconfiguration of addresses, a MN can acquire a unique collocated COA on any foreign link quickly and easily. There is no more need for the FA service and the FA COA type. A MN can have more than one COA (e.g. to support smooth handover), though only the primary COA will be advertised to the HA. The router on the foreign link, which serves the visiting MN is called *access router* (AR).

To obtain a collocated COA for a MN, two methods exists: *stateful* and *stateless address autoconfiguration*. The first includes a server which selects an address from its database for the MN. The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is an example of such a stateful address assignment. In the latter, the address is formed automatically from an interface identifier (e.g. the MN's link layer address) and a valid foreign subnet prefix, both derived from the foreign link, to which the MN is connected.

The Agent Discovery service has been replaced by IPv6 Neighbor Discovery. Similar to Mobile IPv4, *router solicitation* and *router advertisement* (RA) messages exist. Each HA and each MN maintain a list of HAs from which these nodes have received a RA.

A new option is introduced with the dynamic discovery of the HA's address by sending an ICMP *home agent discovery request* message from the MN to the HAs anycast address. Only the closest HA will send the ICMP *home agent discovery reply* message to the MN, including a list of available HAs.

This dynamic HA address discovery allows reconfiguration of nodes on the home link (i.e. replace current router serving as HA by another) even when the MN is visiting a foreign link.

Also, the registration service has been enhanced and renamed. The term *binding* describes the association between the home address of a MN and a

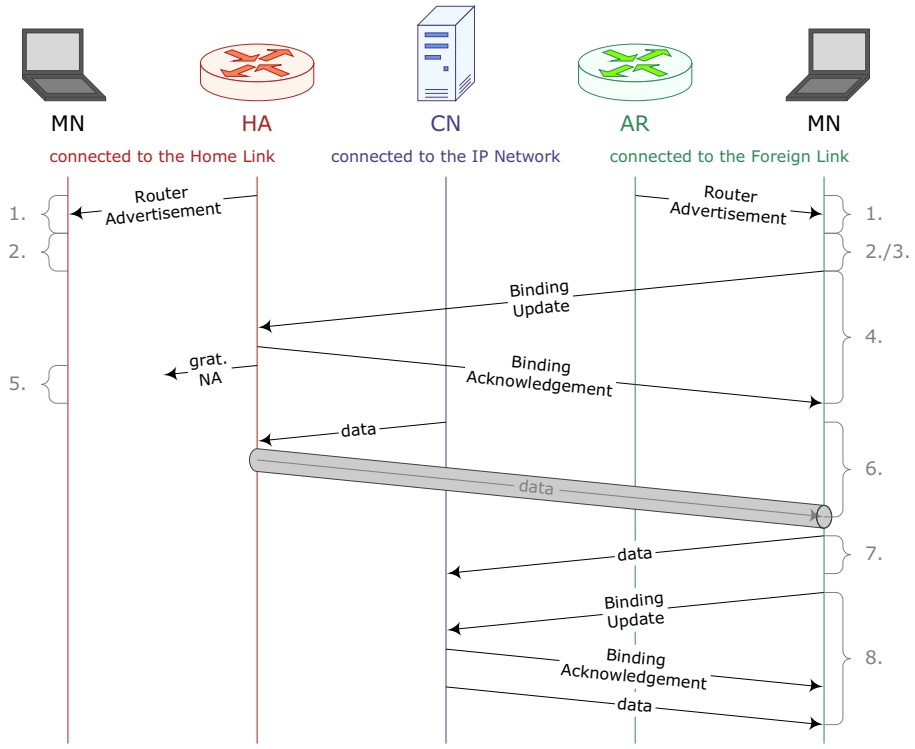

Figure 3.3: Mobile IPv6 operation Time-Message-Diagram

COA. Now apart from HAs, also trusted CNs may receive *binding updates*. It is also possible to request this binding information explicitly from the MN with a *binding request* message.

Mobile IPv6 already integrates route optimization, whereas in Mobile IPv4 it is specified as an additional Internet Draft. Since each MN is assigned at least one COA, direct routing from any CN to any MN becomes possible. There is no need to pass via the home network and the HA, whereby eliminating the triangle routing problem (see Section 5.1.1.1).

3.4.2 Basic operation

A common Mobile IPv6 application flow is shown in Figure 3.3 and described in the following steps.

1. All routers (in this picture HA and AR) broadcast periodically RAs on their respective link.

   (In Mobile IPv6, a RA includes the sender's network prefix or its complete IP address. Additionally, a RA sent from a HA is specially marked.)

2. MNs examine received RAs and decide whether they are connected to their home or a foreign link.

   (MNs connected to their home link just act like stationary nodes.)

3. The MNs connected to a foreign link obtain their collocated COA either through stateless or stateful address autoconfiguration.

4. Now the MN informs its HA about the new collocated COA.

5. The HA sends gratuitous neighbor advertisement messages on its home link to update the neighbor cache of surrounding routers on the same link. This update associates the MN's home address with the HA's link layer address, thereby attracting packets destined for the MN's home address.

6. Upon reception of such packets from a CN, the HA tunnels them to the MN's collocated COA. At the COA (the MN's interface on the foreign link) the original packet is extracted from the tunnel.

7. Any packets sent by the visiting MN are routed directly to their destination (e.g. the CN). Additionally a home address option containing the MN's home address is added to all these outgoing packets.

8. When the CN is trusted, the MN informs the CN about its collocated COA. Now the CN can send its packets directly to the MN using a routing header extension and setting the destination address to the collocated COA.

Chapter 4

Link Layer Handover Statistics

The goal is to determine and validate the Signal-to-Noise Ratio thresholds used by wireless PCMCIA cards to initiate a layer 2 handover as described in Section 2.4.1.

4.1 Preparation

As no standard thresholds have been prescribed each manufacturer uses its own values.

The wireless equipment used in the tests is manufactured by Lucent Technologies' Microelectronics Group [1] and available documentation allowed the verification of the obtained results.

The threshold values for different density settings shown in Table 2.1 are taken from Lucent's Technical Bulletin 023/B [19].

The AP Manager [1] provides a limited control over the threshold values to be used. Three length values (large, medium or small) in the *Distance between APs* field describe the AP density (low, medium or high) of the wireless network.

4.1.1 Equipment

The test equipment consists of two APs (Lucent WavePOINT-II V3.83) and a Laptop acting as the MN, all using WaveLAN cards (Lucent WaveLAN/IEEE Turbo, Firmware 7.52).

[1] now called Agere Systems

A small program called *iwstats* has been written to gather the signal's quality values. These consist of the signal level, noise level and the resulting Signal-to-Noise ratio (SNR). It runs on the MN and logs the accumulated data. Iwstats is based on the Wireless Tools [28] and adds some functionality to let the user specify the length of the gathering period and the interval between the collection of two records. Additionally the output is formated to allow easier evaluation of the data with gnuplot [31].

4.1.1.1 Configuration

The channel setup for the APs provides sufficient channel separation between two APs as described in [17].

The public access to the wireless test network has been disabled using the *Close Wireless System* option in the AP Manager. This feature is non-compliant to the 802.11 standard and implements a stricter handling of association requests (see Section 2.3.3.2) from stations. More information about WaveLAN security options can be found in [20].

Furthermore, all involved APs and the MN have been configured to use the same ESSID. When the Close Wireless System option is activated, a link layer handover can only be carried out between APs and MNs using the same ESSID. The MN can also be configured to connect to any AP by omitting the ESSID specification (i.e. using the value ANY instead) and disabling the Close Wireless System option in the concerned APs.

For a detailed listing of the configuration settings see Appendix A.

4.1.2 Environment

The test site is located under the roof of a brick wall building. The APs have been placed in two separate rooms, connected by a long hall. The first room is used as standard office, the second as test lab and contains therefore lots of technical equipment. The hall in between these two rooms is almost empty.

4.2 Measurements

In accordance with the available AP density settings three series of measurements have been carried out, each consisting of 20 runs. The signal's quality parameters have been gathered at 300 ms intervals.

The roaming took place along the path shown in Figure 4.1. Commencing one meter before the first AP (AP1) the MN moved in front of the second AP (AP2) and from there - following the same path - back to the starting

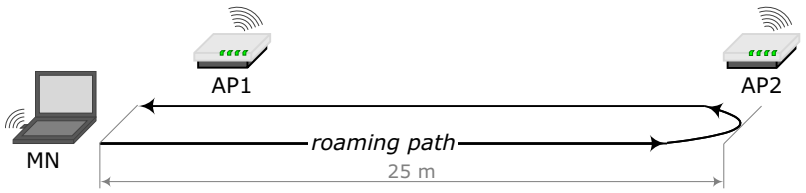

Figure 4.1: Outline of the roaming path

point. With a speed of approximately 3 km/h the distance of 50 meters was covered in about 60 seconds.

The averaged results are graphed in Figure 4.2, 4.3 and 4.4. They illustrate the performance of the signal's quality parameters (signal level, noise Level and SNR) over time.

4.3 Analysis

While moving away from the AP1 the SNR decreases more and more until it reaches the Cell Search threshold. Now the layer 2 handover process (see Section 2.4.1) starts and as result the MN associates with the AP2 and thereby connects to the foreign link. When returning back to the home link, the analogue procedure takes place.

The altering of the handover points throughout the three graphs is due to the changes of the AP density parameter and - at the same time - keeping the experimental setup physically untouched.

Any fluctuations (e.g. local peaks) in the graphs can be most often ascribed to surrounding objects made of interfering material.

4.3.1 Threshold validation

The graphs show that the thresholds listed in Table 2.1 on page 16 are accurate values and will therefore be included in the development process of the mobile-controlled handover (see Chapter 6).

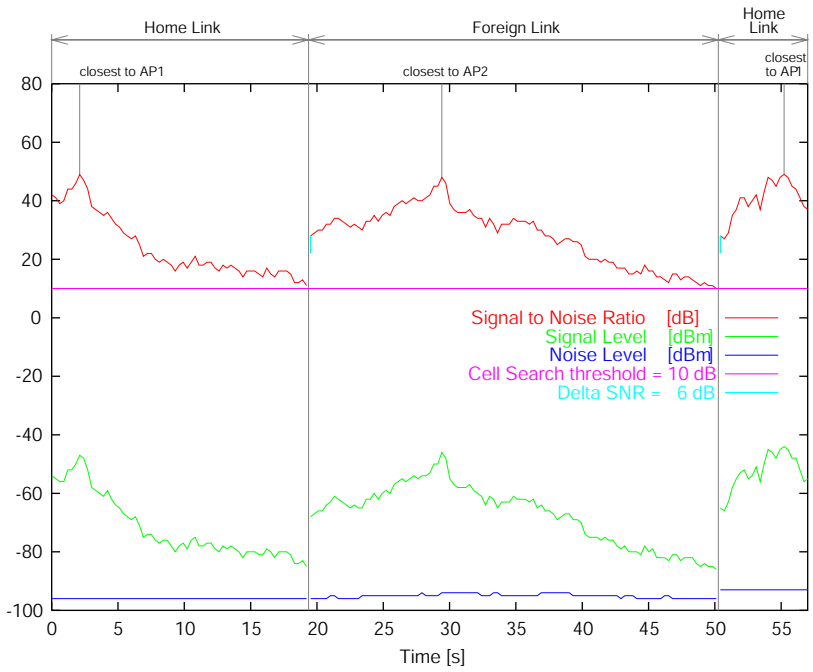

Figure 4.2: Signal to noise ratio when roaming with low AP density

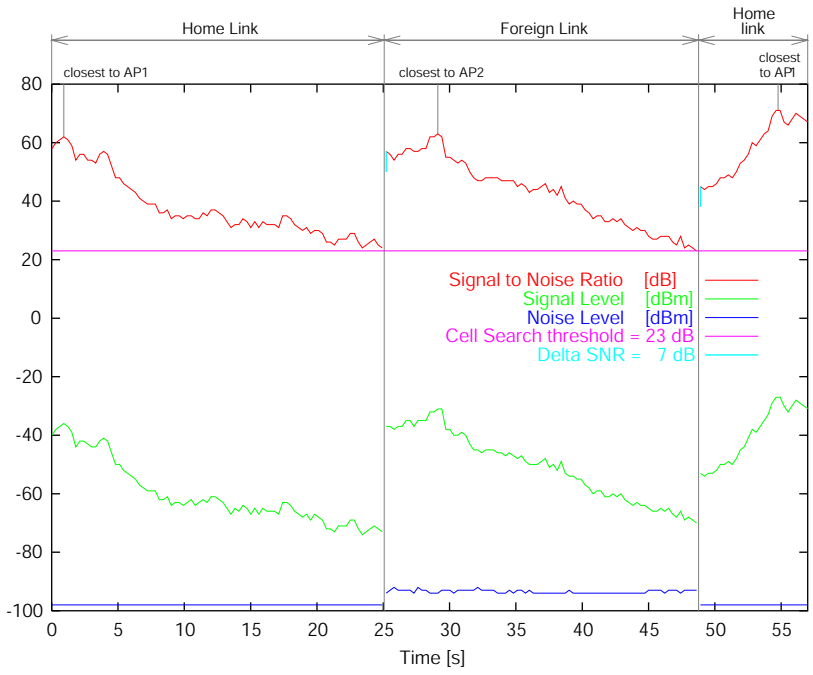

Figure 4.3: Signal to noise ratio when roaming with medium AP density

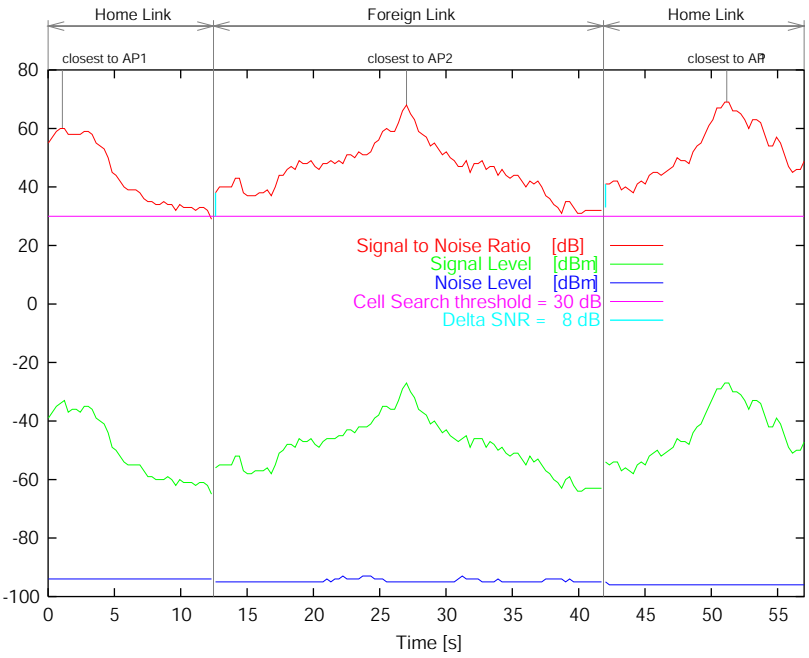

Figure 4.4: Signal to noise ratio when roaming with high AP density

Chapter 5

Mobile-Controlled Handover

With mobile devices becoming more and more popular, suitable solutions for a smooth and fast handover are required. The mobile-controlled handover supports fast handovers, while minimizing the resource usage on a medium with limited bandwidth.

5.1 Motivation

Todays most common mobility solutions provide support for either macro-mobility (IETF Mobile IP, see Chapter 3) at the network layer or micro-mobility at the link layer level (IEEE 802.11, see Section 2.3).

Although these two standards cover certain areas of mobility application, the interworking between both of them needs further development.

One of the major concerns has been and still is the *seamless handover* in IP networks. The term *seamless* describes a change of location (e.g. connecting to a new AP on a foreign link at large distance [in terms of delay] from the home link), that is (almost) imperceptible by the user of the MN. This requires both, a smooth (low data loss) and fast (small delay) handover.

Mobile IP allows roaming between various subnetworks by acting like a routing protocol. Several problems regarding the handover process have been identified since its specification. In Section 5.1.1, three of them are described in detail.

Of course, involved groups and researchers have already thought about these problems and proposed solutions (see Section 5.3). Most of them operate at the network layer level only and produce additional (short high peak) network traffic (e.g. via buffering mechanisms). This reduction in resources can not be neglected on the wireless medium, where bandwidth still is short in supply.

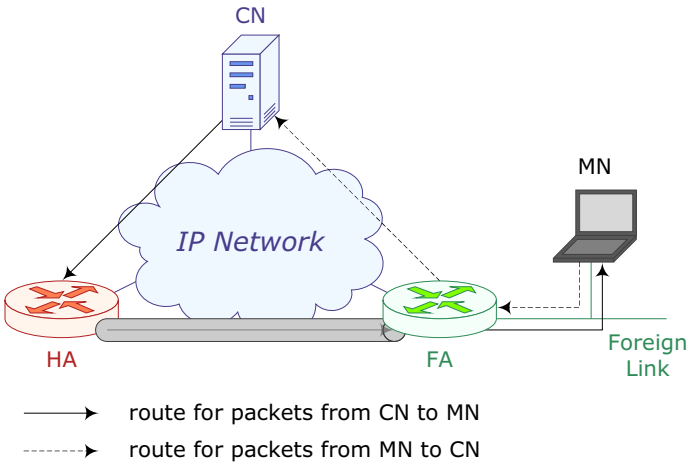

Figure 5.1: Sub-optimal triangle routing

The idea is to react in due time to changes in location of the MN and thus allow suitable preparations to be made by network management entities for a fast handover.

5.1.1 Handover issues

During the implementation and application of the Mobile IP standard, it became apparent that the handover process was not operating satisfactory under some common conditions.

The following problems are independent of each other, but their effects can accumulate.

5.1.1.1 Triangle routing

Packets destined for the MN have to be sent to the HA in the first place, and are then tunneled to the current FA, which delivers them to the MN. This triangle route may be in many cases sub-optimal as shown in Figure 5.1 and therefore lead to unnecessary delays.

5.1.1.2 Out-of-date location information

While the handover is carried out, already tunneled packets are lost and need to be retransmitted, because their destination address (i.e. the MN's COA) is no longer valid. This causes noticeable delays.

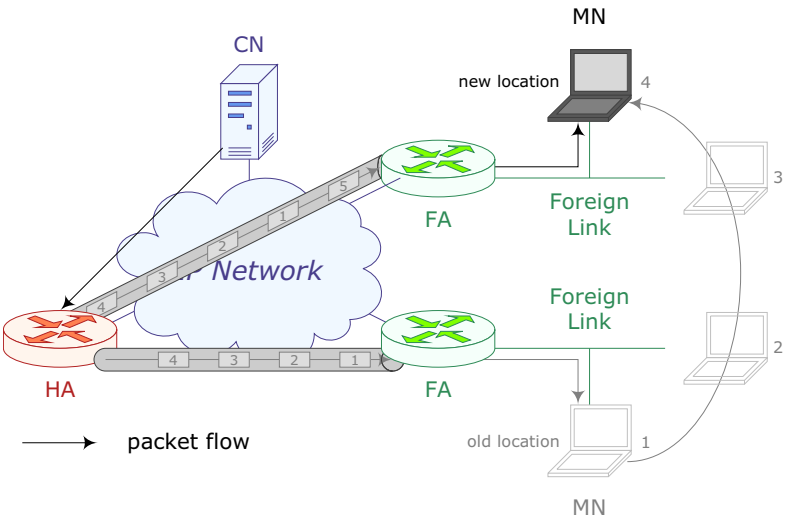

Figure 5.2: Out-of-date location information causing packet loss

Additionally this packet loss activates TCP's congestion control mechanisms, which among other things start to limit the bandwidth. This is in no way desirable since the actual reason for the packet loss is not the assumed network congestion.

Figure 5.2 illustrates a handover, where the HA becomes aware of the change in location only after the fourth packet has been tunneled to the old COA. The FA now gets an out-of-order packet (sequence number 5) and alerts the sender (CN). The four previously transfered packets are retransmitted to the new COA.

5.1.1.3 Frequent handovers

In an area of high AP density and many FAs (i.e. many APs with small cells, while each AP covers its own subnetwork), frequent handovers result in a lot of additional administrative overhead caused by the process of de-/registration with the FAs and updating the HAs with the new COA for each handover.

5.2 Concept

The underlying concept assumes that a change of location always directly affects the signal quality. Thus, observing these values gives information about the MNs movements.

Moreover, a scan (see Section 2.3.3.1) for surrounding APs reveals potential new association targets for the MN. These possible targets will be advertised to concerned entities (e.g. QoS-Manager) in due time, so they can take appropriate actions.

It is important to note, that the original layout of the scan procedure had to be changed because of difficulties related to the hardware control (see Section 5.2.2.1).

These encountered restrictions lead to incisive consequences. Each AP needs to be assigned a unique wireless cell name (i.e. ESSID) and the program must be informed in advance about it's surrounding APs by transferring their ESSIDs.

Nevertheless, the following feature of IEEE 802.11 compliant hardware is very useful. The assignment of a specific ESSID to the MN will only allow the association with an AP using the very same ESSID.

Due to the predefined one-to-one relation between ESSIDs and APs, the successive switching of ESSIDs on the MN forces the handover and allows the gathering of the signal's quality parameters for each of the ESSIDs.

As this solution works on the link layer level, it does not interfere with Mobile IP, which operates at the network-layer. In fact, this concept supports the fast handover process, by providing means of control over and synchronization with the handover procedure.

5.2.1 Conceptual operation

The operational design is based on a program which provides services to entities in need for them. This allows other programs (service users) to directly supervise the handover process and immediately obtain the results.

The service user sends a list of available wireless cells (i.e. ESSIDs) to the service program.

The service program itself resides on the MN and constantly monitors the signal quality (see Section 2.4.2) of its current wireless link.

It reacts upon a change of these values (e.g. falling below a threshold) and alerts the affected service user. The service user in turn orders the search for potential new links. The service program queries the surrounding APs by their provided ESSIDs and sends the results to the service user.

Next the service user can dispose the change to the new location with a certain delay. Having performed the change, the service program informs the service user about the results.

It then continues to monitor the link quality, waiting for the next threshold shortfall to occur.

The service user can send a new list of wireless cells to the service program at any time to adjust to a changing environment.

5.2.2 Alternative schemes

In the early stages many solutions were considered, but later found to be impracticable and thus not pursued any longer.

5.2.2.1 Original concept

The original concept required good control over the wireless LAN hardware. Unfortunately, due to undesirable firmware behavior and the lack of powerful drivers, caused by restrictive hardware company policies, it had to be severely limited.

The basic idea was to have a program which is able to initiate firmware functions. The MN's association with a specific AP could be maintained and it would be possible to use the channel sweep (see Section 2.4.1) method to gather the signal's quality parameters from all surrounding APs in very short period.

The program wouldn't require any information about the currently visited network and could therefore have a more general range of use.

In reality, the firmware of the wireless LAN card could not be forced to stay associated with a certain AP, which lead to the decision to introduce the one-to-one relation between APs and ESSIDs instead of using a common ESSID for all APs.

But the wireless LAN hardware drivers under Linux were unable to provide the signal's quality parameters from APs using an ESSID different from the MN's current ESSID. An inquiry with the authors of the Wireless Tools [28] and the Orinoco [10] driver ascribed this to the lack of available documentation for the respective hardware. Therefore, the switching of ESSIDs to gather the signal quality from all APs had to be applied.

5.2.2.2 WaveLAN MIB and SNMP

After having discovered the problems described above, SNMP (Simple Network Management Protocol) was examined too.

Most networking devices (such as APs) use a MIB (Management Information Base), which contains relevant system variables. These can be accessed and altered via SNMP. The variables are represented by numbers. However, without the MIB definition from the used hardware, it is guesswork to associate numbers to variables.

The 802.11 MIB definitions do not contain the necessary information (signal's quality parameters) and no definition for the WaveLAN MIB is publicly available at the time of writing. Anyhow, a small utility [21] was found, which resolves a great part of the WaveLAN MIB numbers.

Nevertheless, design issues (e.g. evaluating the quality information from all APs at a centralized point) and the sometimes unreliable retrieval of the signal's quality parameters led to the suspension of further investigation in this area.

5.3 Related work on handover improvements

As mentioned before, the solutions currently proposed operate at the network layer. They either specify smooth or fast handover mechanisms.

5.3.1 Mobile IPv4 extensions

During the specification and application of the Mobility Support in IPv4 [23] many flaws have been discovered and solutions proposed.

5.3.1.1 Optimized Smooth Handoffs

In [26] the problems of triangle routing, out-of-date location information and frequent handovers are addressed. This document summarizes existing papers and introduces new concepts.

To solve the triangle routing problem, route optimization as described in [25] is used. A binding cache is maintained in any host willing to participate. As soon as the HA receives a packet for a MN being out, it sends a binding update, containing the MN's current COA, to the source of the packet. The source updates its binding cache and tunnels ensuing packets for the MN directly to its COA.

A buffering mechanism minimizes the packet loss caused by out-of-date location information. Every FA uses a buffer, where it keeps a limited number of already forwarded packets for the MN. When a handover occurs the MN registers with a new FA, which in turn requests the transmission of the buffer from the previous FA. To eliminate duplicate packets, the MN buffers information (source address and identification) about received datagrams. It includes these receipts in the registration request for the new FA, which forwards them to the old FA together with the transmission request of the buffer. Now the old FA can determine which packets have been lost during the handover and send them to the new FA.

The administrative overhead resulting from frequent handovers is reduced with a hierarchical FA management scheme. All FAs are organized into a tree, so that local movements of the MN can be handled faster within the domain. To be more precisely, only FAs along the path to the lowest common node (another FA) of the old and the new FA are affected by a handover.

5.3.1.2 Low Latency Handoffs

The proposal found in [7] defines pre- and post-registration mechanisms and link layer triggers. The main idea is based on the make-before-break concept. The authors aim to reduce the latency caused by the Mobile IP registration process, thus allowing fast handovers.

The layer 2 triggers are used to signal important events (e.g. announcing a future link layer handover, link up or link down) occurring at the link layer level to the network layer.

In the pre-registration method, the MN first completes the layer 3 registration process with the new FA and then changes to the new FA's link.

Upon the announcement of a future link layer handover by a layer 2 trigger the old FA sends cached agent advertisements from surrounding FAs to the MN. The MN chooses a new FA and registers with it via the old FA. After successful registration with the new FA, the layer 2 handover is performed (i.e. the MN changes to the new FA's link).

When using the post-registration method, the link layer handover procedure is completed normally, but the MN stays registered with the old FA until it decides to register with the new FA on the current link or to change to another link.

After the MN has registered with the old FA, the old FA becomes the mobility anchor point for the MN, called the anchor FA. At the reception of a layer 2 trigger indicating a future link layer handover, a bidirectional tunnel between the anchor and the new FA is established. As soon as the link to the MN goes down, the anchor FA starts forwarding MN-bound packets to the new FA via the tunnel. When the link goes up again (i.e. the MN is connected to the new FA's link), the MN receives the tunneled packets from the anchor FA. Now the MN can decide to register with the new FA or to change the link again. Either way, the bidirectional tunnel between the anchor and new FA will be removed. In the latter case, a new bidirectional tunnel between the FA on the new link and the anchor FA may be established (depending on the wireless system used). Again, the MN needs to choose between registration or link change.

Additionally a combination of pre- and post-registration handovers is described. First the pre-registration method is performed and if it does not

complete within a specified period, the post-registration method will be executed.

5.3.2 Mobile IPv6 extensions

Since the ratification of the Mobility Support in IPv6 [16] is still in progress, many Internet-Drafts suggesting handover improvements have been published.

5.3.2.1 QoS-Aware handover

The approach described in [4] introduces an additional handover trigger. Instead of only waiting for the signal quality to drop below a certain threshold, the MN regularly searches for new links offering better resources.

Before the handover is executed, the MN checks the availability of resources on the new link. Only if the current sessions can be uphold, the MN performs a handover. Otherwise, the current link is maintained.

The authors work with several assumptions. The MN can access more than one link layer technology at the same time. The QoS signaling is done via RSVP (Resource ReSerVation Protocol [3]). A secondary HA is installed in a node at the border to the public network (containing the CN). The secondary HA is responsible of forwarding the chosen PATH and RESV messages.

Upon start of a QoS-aware handover process, the MN announces this ongoing process to the secondary HA, so that the secondary HA can handle the following PATH and RESV messages correctly.

Shortly after, the MN sends PATH messages both on the old and the new link to the receiver (CN). After having passed several RSVP capable routers, these messages arrive at the secondary HA. Now the secondary HA forwards the PATH message with the worst deviation parameters, i.e. the PATH message that will provoke the largest bandwidth reservation along the data path.

After the reservation has been evaluated by the receiver (CN), a RESV message, including the bandwidth to be allocated, is sent back along the path. This bandwidth is always the highest value from both the old and the new, yet to be reserved bandwidth. This ensures that the former reservation along the old path will not break and can be maintained in case the handover to the new link fails. A possible resource waste will be corrected by future PATH/RESV messages between the MN and the CN.

When the RESV message arrives at the secondary HA, it is forwarded to the new link only. At the same time, the old RESV message is send to the old link, to keep the former reservation alive.

The MN now receives both RESV messages and checks the resource availability on the interface towards the new path. If the resource has been reserved, the MN may perform a QoS-aware handover. Otherwise, it keeps the former reservation on and connection to the old link.

5.3.2.2 Fast Handovers for Mobile IPv6

The document [6] specifies protocol enhancements in the style of the make-before-break concept to reduce the handover latency.

The authors explicitly state that only scenarios are covered, wherein the MN can initiate a layer 3 handover while it still has layer 2 connectivity to the current AR. Additional prerequisites are the ability of an AR to derive the IP address of an neighboring AR from the link layer address of an attached AP and the existence of link layer triggers indicating MN movements.

This proposal lets the MN configure a new collocated COA before it moves to the new AR. Upon connection with the new AR, the MN can instantly use this collocated COA. If the MN is unable to obtain a new collocated COA in advance, it can also continue to use the old COA, even after being connected to the new AR.

To enable such a design, several new messages have been implemented between ARs and between an AR and a MN.

The fast handover process is initiated by the MN, when it sends a router solicitation for proxy message to the old AR to ask for a fast handover to a new point of attachment. In this message, the MN puts an identifier of the new point of attachment it is going to move to. The old AR responds with a proxy router advertisement message. If new the point of attachment is known to the old AR, the message will contain the prefix to form the new collocated COA or the new collocated COA itself.

Moreover, the old and the new AR also exchange information. With the handover initiate message the old AR requests the new AR to validate or provide a collocated COA. The new AR replies with the handover acknowledgment message either accepting or rejecting the collocated COA, suggested from the old AR or the new AR provides a collocated COA.

Before the MN executes the handover, it sends a fast binding update message on its old link. Upon reception of that message by the old AR, it will form a temporary tunnel to the new collocated COA, through which the old AR will send the fast binding acknowledgment. The same message will be sent to the MN on the old link.

If now new collocated COA can be determined, the old COA will be temporary hosted by the new AR. A tunnel between the old and new AR will be established to forward packets destined for the MN.

As soon as the MN moves to the new AR, the MN announces its arrival with a fast neighbor advertisement message to initiate the delivery of packets.

Chapter 6

Implementation

This chapter describes the implementation process of the mobile-controlled handover concept, including detailed information about the communication interface.

6.1 Background

The handover control mechanisms are used by the mobile client of a bandwidth broker, in order to allow the updating of the network configuration in due time. The bandwidth broker itself uses Differentiated Services to provide QoS for Mobile IP.

6.2 Design requirements

When specifying the software functionality, several aspects have to be taken into account.

To allow mobile-controlled handover and in-time preparation, direct access and control over the wireless LAN hardware from the monitoring program is necessary.

At first sight this implicates the integration of hardware-specific components, but a generalized interface to any wireless LAN hardware is provided with the *wireless extensions* under Linux. Of course, these extensions must be supported by the hardware driver.

Also, the monitoring program needs to run as background process (daemon) on the MN.

Furthermore it must provide means of communication with the mobile client of the bandwidth broker. The bandwidth broker's mobile client too resides on the MN.

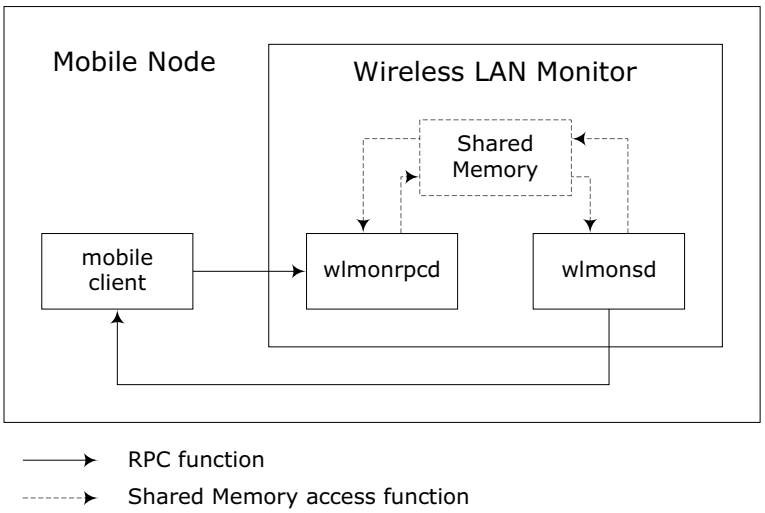

Figure 6.1: Interaction of the Wireless LAN Monitor components

These requirements lead to several assignments covering interprocess communication (IPC) and other system programming topics.

6.3 Wireless LAN Monitor

The programming work of this thesis is released under the name *Wireless LAN Monitor* [29]. The implementation was done in C++ under Linux, using the C++ Standard Library.

The Wireless Tools [28] have been used as a reference for the wireless LAN hardware access functionality.

6.3.1 Basic design

The Wireless LAN Monitor has been split into two daemons (*wlmonrpcd* and *wlmonsd*). The first provides the data transmission from the bandwidth broker's mobile client to the Wireless LAN Monitor, the latter is responsible for the data transmission to bandwidth broker's mobile client and for the monitoring the signal's quality parameters of the mobile node, where all three programs are running on (see Figure 6.1).

To exchange data between the two daemons the shared memory concept is used. The communication between the Wireless LAN Monitor's components and the mobile client of the bandwidth broker has been realized via remote procedure calls (RPCs). Figure 6.2 illustrates the implemented IPC functions and their use in the components of the Wireless LAN Monitor.

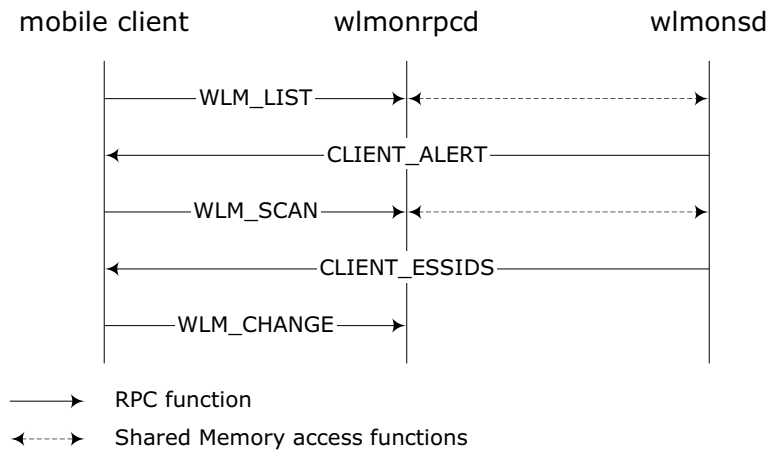

Figure 6.2: Wireless LAN Monitor IPC functions

position	data type	description
0	*int*	number of ESSID names
1	*char* ∗	ESSID name 1
⋮	⋮	⋮
n	*char* ∗	ESSID name n

Table 6.1: WLM_LIST parameter field

6.3.2 Wireless LAN Monitor RPC Daemon

The wlmonrpcd acts as RPC server and forwards orders sent by the bandwidth broker's mobile client to the wlmonsd, which executes them. It is started and terminated by the wlmonsd.

6.3.2.1 Communication interface definition

The following RPC functions are provided by the wlmonrpcd. For each function the purpose and the expected parameters are specified.

- WLM_LIST (parameter field format in Table 6.1)

  This function transfers a list of ESSID names. First the number of included ESSIDs is passed and then the ESSIDs themselves.

- WLM_SCAN (no parameters)

position	data type	description
0	*int*	index representing an ESSID name
1	*int*	delay to wait before switching

Table 6.2: WLM_CHANGE parameter field

position	data type	description
0	*int*	number of ESSID list indices
1	*char* $*$	ESSID list index 1
$\vdots$	$\vdots$	$\vdots$
n	*char* $*$	ESSID list index n

Table 6.3: CLIENT_ESSIDS parameter field

To initiate a scan for new, better serving APs, WLM_SCAN has to be called without any parameters.

- WLM_CHANGE (parameter field format in Table 6.2)

  Calling this function invokes a change of the current ESSID. The first parameter is an index of the original ESSID names list, representing the new ESSID to change to. The second parameters describes the time to wait before executing the change.

6.3.3 Wireless LAN Monitor Service Daemon

The wlmonsd represents the main program. It monitors the signal quality and takes appropriate actions as necessary.

6.3.3.1 Communication interface definition

The service daemon calls the following RPC functions, which are provided by the mobile client of the bandwidth broker.

- CLIENT_ALERT (no parameters)

  To alert the bandwidth broker's mobile client about a signal quality drop, this function is executed.

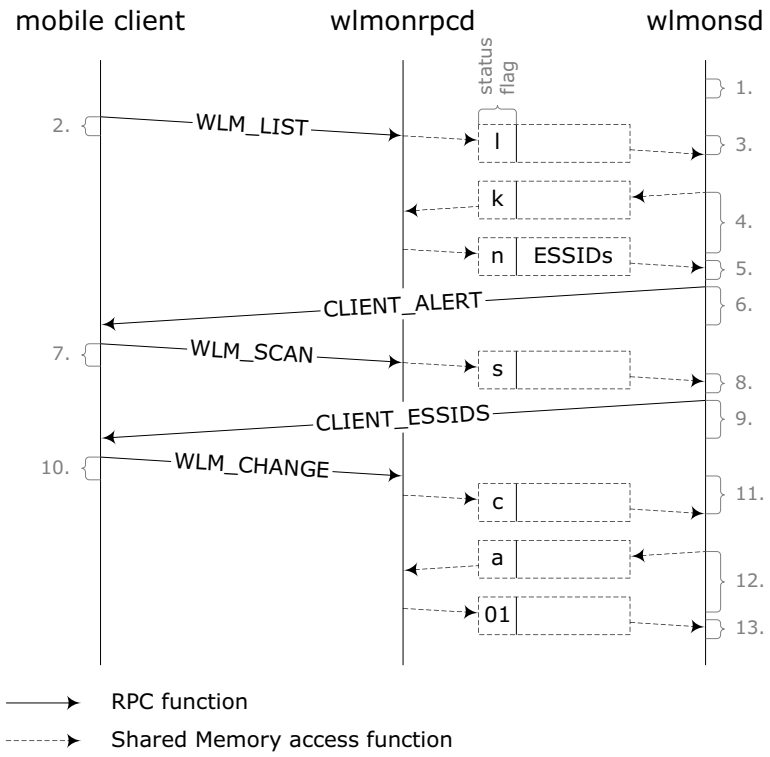

Figure 6.3: Wireless LAN Monitor procedure message-time diagram

- CLIENT_ESSIDS (parameter field format in Table 6.3)

  This function transfers a list of ESSID indices. First the number of included indices is passed and then the indices themselves.

6.3.4 Wireless LAN Monitor operation

The cycle of the Wireless LAN Monitor's components interacting with the mobile client of the bandwidth broker are described with the following steps and illustrated in Figure 6.3.

To synchronize the shared memory access of the wlmonsd and the wlmonrpcd the first character in the shared memory field has been turned into a status flag.

1. When the Wireless LAN Monitor Service Daemon (SD) is started, it invokes the Wireless LAN Monitor Remote Procedure Call Daemon (RPCD).

2. The bandwidth broker's mobile client (BBMC) passes an ESSID list to the RPCD.
3. After reception, the RPCD requests the transfer of the list to the SD.
4. The SD acknowledges the request and hereon the RPCD places the list into the shared memory and confirms the transfer's completion.
5. Having awaited the confirmation, the SD now reads the list from the shared memory.
6. Assuming that the signal quality falls below the predefined threshold (e.g. because the MN may have moved), the SD alerts the BBMC.
7. Next the BBMC sends an order to scan for better serving APs to the RPCD, which in turn places a specific mark in the shared memory to be read by the SD.
8. The SD becomes aware of the request mark and starts to scan other wireless cells identified by their ESSID from the list.
9. After finishing the scans, the SD informs the BBMC about the results by passing a list of indices. Sorted descending by signal quality, each index represents an ESSID from the original list submitted by the BBMC.
10. The BBMC sends an order to change the wireless cell with a certain delay to the RPCD.
11. After having waited for the specified delay, the RPCD announces the requests to change to the SD.
12. When the SD acknowledges the request, the RPCD puts the index, to which the SD should change to, as unsigned character in the shared memory.
13. The SD reads the index and carries out the change of the ESSID.

Chapter 7

Application

During the application phase the Wireless LAN Monitor has been examined in the test lab. The duration of the communication disruption during a scan to obtain the signal's quality parameters has been of particular interest.

7.1 Test environment

A specifically designed test environment has been built up in the lab to study the Wireless LAN Monitor's functionality in practice. Figure 7.1 shows the test scenario. Appendix A contains the detailed configuration settings.

7.1.1 Hardware

Three APs (Lucent WavePOINT-II V3.83) have been deployed on the same floor, one connected to the home and two to the foreign link. Two PCs act as boundary routers for their respective (home and foreign) networks. A switch (Cabletron SmartSwitch 6000) provides the interconnection between the network components. The home and the foreign network have been simulated using virtual LANs (grouped ports) on a switch module (6H252-17). A laptop acts as the mobile device. All wireless components (APs, laptop) use WaveLAN cards (Lucent WaveLAN/IEEE Turbo, Firmware v7.52).

7.1.1.1 Settings

The APs use the following channels: AP1 on 2412 MHz, AP2 on 2472 MHz and AP3 on 2442 MHz. Thus, the frequency separation between the channels of the APs exceeds the required 25 MHz (for flawless operation as described in [17]). Each AP uses a unique ESSID (Wireless Cell 1, 2 and 3).

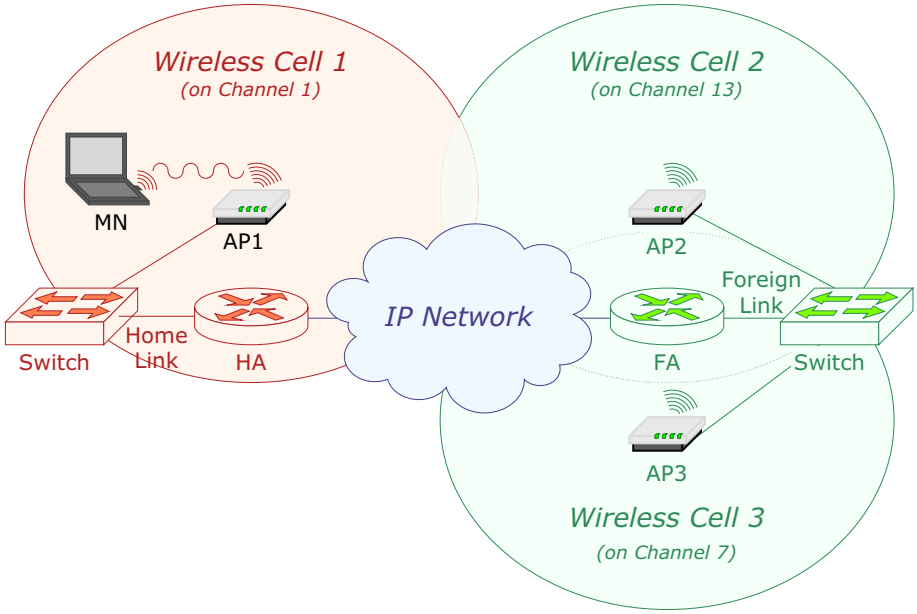

Figure 7.1: Test environment

7.1.2 Software

All PC systems (boundary routers, laptop) run Debian/GNU Linux (v2.2r4) with the Linux kernel (v2.2.20). On the laptop the PCMCIA card service (v3.1.30) and the Wireless Tools [28] (v22) have been installed. From the PCMCIA card service package the Orinoco [10] driver (v0.08) has been chosen for the WaveLAN card. As Mobile IPv4 implementation Dynamics [11] (v0.8.1) has been used. The HA and the FA daemons run on the two boundary routers respectively, the MN daemon operates on the laptop. Also, the Wireless LAN Monitor runs on the laptop.

7.1.2.1 Configuration

The Linux kernel has been updated with the wireless extensions (v12) provided by the Wireless Tools. Dynamics has been configured to preferably use a reverse tunnel (instead of a triangle tunnel) and to send out agent advertisements every 5 seconds. The Wireless LAN Monitor has been configured to use the standard thresholds (see Section 2.4.3).

During the Wireless LAN Monitor's operation it became apparent, that either the WaveLAN driver or the Linux kernel needed some time to reflect the change of the ESSID and update the singal's quality parameters to the actual values. Therefore, a configurable parameter, which states the delay

handover type	inter-domain (COA change)		intra-domain (no COA change)
change in the link layer attachment	AP1 (on the home link) → AP2 (on the foreign link)	AP2 (on the foreign link) → AP1 (on the home link)	AP2 → AP3 (both on the same foreign link as the FA)
duration [s]	$15 - 20$	$5 - 7$	≈ 1

Table 7.1: Mobile IPv4 handover duration

between the change of ESSIDs, has been introduced. Currently it is set to 200 ms.

7.2 Results

The disruption of the communication at the network layer level caused by the scan process (switching ESSIDs) has been investigated.

The scan process itself operates at the link layer level. As mentioned above, the time until the kernel or the driver become aware of the ESSID change and allow the gathering of the signal's quality parameters varies between 150 and 200 ms.

However, the Mobile IP handover process operates at the network layer and its time to completion depends on the type of handover the MN is engaged in. Table 7.1 shows the duration for three handover types. These values have been measured while sending UDP traffic from a CN to the MN.

7.2.1 Communication disruption

A scan process causes a period of communication disruption which scales linearly with the number of wireless cells to scan. The following equation describes the total time of communication disruption during a scan process: $t_{communication\ disruption} = n_{\#\ cells} * t_{ESSID\ change\ delay}$.

The values from Table 7.1 indicate that there is no time of establishing a connection on the network layer between the switching of ESSIDs, because the Mobile IP registration process takes too long.

The number of usable frequency channels within a small environment ($5 - 10$ m radius) is limited to three. The thereby provided channel separation is large enough to guarantee that the signals will not interfere with each other.

It is of course possible to use the same frequency channels again outside of this small environment.

However, the MN can receive the signal properly only from APs close to it. Thus, the bandwidth broker's mobile client should update the ESSID list of the Wireless LAN Monitor frequently and keep its size as small as possible (by removing the ESSIDs of APs, from which the MN is not able to receive a signal). This would require some topological database (e.g. a neighbor list for each AP).

In the ideal case, the MN would always have the ESSIDs of the actual three closest surrounding APs, causing the scan process to interrupt communication for 600 ms (with the ESSID change delay set to 200 ms).

Chapter 8

Summary and Outlook

8.1 Summary

The concept of the solution proposed in this thesis shows many great advantages, that is, it provides the necessary instruments to monitor and control the handover process without adding new extensions to the already existing Mobile IP standard. Instead it uses what already exists, the quality parameters of the wireless link and the wireless LAN hardware's specification. The first is accessible through the driver, the latter may be more complicated to obtain.

Nevertheless, the usage of the SNR as parameter that is common to all wireless LAN hardware, makes it a rather flexible design. Although the adjustment of the thresholds to the hardware vendor's specific values remains, this task could be avoided by using relatively high thresholds (adding 5 dB to the Cell Search thresholds used herein, see Section 2.4.3). This would increase the amount of handovers on a reasonably planned AP installation only little and offer a more universal area of application.

The implemented communication interface permits other applications (i.e. service user) to take over the handover process control. Including this functionality, the concept of this thesis can be seen as integral part of a fast handover solution.

For example, when a service user orders the handover to be performed by the Wireless LAN Monitor, the service user also indicates a lag value. The Wireless LAN Monitor will defer the handover for the given delay. During this time, the service user can execute all necessary network management functions for a fast handover.

In the thesis' usecase, the service user has been represented by the mobile client of a bandwidth broker. This mobile client will calculate new registrations in synchronization with the bandwidth broker during the delay

mentioned above. Thus, when the handover completes, the flow will already have been mapped to the mobile node's new point of attachment. This approach enables a fast handover process.

Furthermore, other entities, which do not reside on the mobile node itself, can take advantage of the provided handover control. An example would be a smooth handover procedure which involves the buffering of a certain amount of packets at the current point of attachment (i.e. the current AR). When the handover has been ordered by the mobile client of the bandwidth broker, the Wireless LAN Monitor could trigger the forwarding of the buffered packets from the old to the new point of attachment. This would require a very small addition (e.g. one function call) to the Wireless LAN Monitor.

In its current state the Wireless LAN Monitor enables fast handovers, but can be easily extended to support smooth handovers at the same time, thereby allowing seamless handovers.

8.2 Outlook

Most of the Mobile IP extensions can be divided into two categories: either they aim to support fast or smooth handovers. To date, no proposal exists that implements both, fast and smooth handovers (i.e. seamless handover) at the same time.

An effort into this direction lead the foundation of the SeaMoby Working Group [12]. One of the group's goals is the definition of a common signaling protocol which allows the transfer of authentication, authorization and accounting (AAA) information between IP nodes. The SeaMoby working group's work is still in it's very early stages.

It is clear that the problems (e.g. lack in hardware documentation) encountered during the specification and implementation phase lead to some incisive restrictions. The most troublesome certainly is the very slow scan process (recognizing the new ESSID can take up to 160 ms) and the need of information about the surrounding network topology in advance.

During the very end of the work on this thesis a modified (through reverse engineering) version [32] of Lucent's WaveLAN driver for Linux has been published. This driver allows the gathering of the signal quality from all APs in range at the same time via the active scanning function of the wireless LAN hardware. This would enable the original concept and lead to much faster response times. It is to say, that the author of the modified driver choose to define its own API instead of integrating his work into the already existing and established drivers, making the compatibility and future of his work uncertain.

Appendix A

Configuration

A.1 General Settings

```
IBM ThinkPad 380ED
------------------
Name:                                    pioneer
IP:                                    10.1.1.100
                                      130.92.70.47
Subnet Mask:                         255.255.255.0
wvlan0:      MAC:                 00:60:1D:04:32:D6
        Firmware:                             7.52


MN DELL Latitude CPi
--------------------
Name:                                      sapwood
IP:                                     10.1.1.99
                                      130.92.70.49
Subnet Mask:                         255.255.255.0
wvlan0:      MAC:                 00:60:1D:04:2E:24
        Firmware:                             7.52


WC1  WavePoint-II  (Home Network)
-----------------
Name:                                    AP_Cell_1
Description:                    WavePOINT-II V3.83
wvlan0:      MAC:                 00:60:1D:04:2E:25
        Firmware:                             7.52
eth0:        MAC:                 00:60:1D:03:DA:23
```

```
-+-*Wireless Interfaces
 | |
 | +-*PC card slot A
 |   |
 |   +-Network Name:                Wireless_Cell_1
 |   |
 |   +-*Wireless Advanced Setup
 |   | |
 |   | +-Channel/Frequency:             1/2.412 GHz
 |   | +-Distance Between APs:                Large
 |   | +-Multicast Rate:                    2 Mbit/s
 |   |
 |   +-*Wireless Security Setup
 |     |
 |     +-Close Wireless System                  Yes
 |
 +-*Access Point IP
 | |
 | +-*Specify an IP address
 |   |
 |   +-Access Point IP Address:            10.1.1.5
 |   +-Access Point Subnet Mask:      255.255.255.0
 |   +-Default Router IP:
 |
 +-*SNMP
 | |
 | +-System Name:                          AP_Cell_1
 | +-SNMP IP Access List
 |     Address   Mask           Interface
 |     10.3.1.0  255.255.255.0  X
 |     10.3.2.0  255.255.255.0  X
 |
 +-*Access Control
 | |
 | +-Setup Access Control
 |     MAC Address        Comment
 |     00:60:1D:04:2E:24  MN WaveLAN card
 |     00:60:1D:04:2E:25  WC1 WaveLAN card
 |     00:60:1D:04:2E:26  WC2 WaveLAN card
 |     00:60:1D:04:32:96  WC3 WaveLAN card
 |     00:60:1D:04:32:D6  tmp WaveLAN card
 |
```

```
 +-*Ethernet Interface
   |
   +-10 Mbit/s Full Duplex (Twisted Pair Port)  Yes


WC2  WavePoint-II  (Foreign Network)
-----------------
Name:                                    AP_Cell_2
Description:                      WavePOINT-II V3.83
wvlan0:      MAC:                  00:60:1D:04:2E:26
        Firmware:                                7.52
eth0:        MAC:                  00:60:1D:F4:40:2C


-+-*Wireless Interfaces
 | |
 | +-*PC card slot A
 |   |
 |   +-Network Name:                Wireless_Cell_2
 |   |
 |   +-*Wireless Advanced Setup
 |   | |
 |   | +-Channel/Frequency:            13/2.472 GHz
 |   | +-Distance Between APs:                Large
 |   | +-Multicast Rate:                   2 Mbit/s
 |   |
 |   +-*Wireless Security Setup
 |     |
 |     +-Close Wireless System                 Yes
 |
 +-*Access Point IP
 | |
 | +-*Specify an IP address
 |   |
 |   +-Access Point IP Address:            10.1.2.5
 |   +-Access Point Subnet Mask:      255.255.255.0
 |   +-Default Router IP:
 |
 +-*SNMP
 | |
 | +-System Name:                           AP_Cell_2
 | +-SNMP IP Access List
 |     Address   Mask           Interface
 |     10.3.1.0  255.255.255.0  X
```

```
 |     10.3.2.0  255.255.255.0  X
 |
 +-*Access Control
 | |
 | +-Setup Access Control
 |     MAC Address        Comment
 |     00:60:1D:04:2E:24  MN WaveLAN card
 |     00:60:1D:04:2E:25  WC1 WaveLAN card
 |     00:60:1D:04:2E:26  WC2 WaveLAN card
 |     00:60:1D:04:32:96  WC3 WaveLAN card
 |     00:60:1D:04:32:D6  tmp WaveLAN card
 |
 +-*Ethernet Interface
   |
   +-10 Mbit/s Full Duplex (Twisted Pair Port)  Yes


WC3  WavePoint-II  (Foreign Network)
-----------------
Name:                                    AP_Cell_3
Description:                      WavePOINT-II V3.83
wvlan0:      MAC:                  00:60:1D:04:2E:26
        Firmware:                              7.52
eth0:        MAC:                  00:60:1D:F4:40:2C


-+-*Wireless Interfaces
 | |
 | +-*PC card slot A
 |   |
 |   +-Network Name:                Wireless_Cell_3
 |   |
 |   +-*Wireless Advanced Setup
 |   | |
 |   | +-Channel/Frequency:             7/2.442 GHz
 |   | +-Distance Between APs:                Large
 |   | +-Multicast Rate:                    2 Mbit/s
 |   |
 |   +-*Wireless Security Setup
 |     |
 |     +-Close Wireless System                  Yes
 |
 +-*Access Point IP
 | |
```

```
| +-*Specify an IP address
|   |
|   +-Access Point IP Address:            10.1.2.6
|   +-Access Point Subnet Mask:      255.255.255.0
|   +-Default Router IP:
|
+-*SNMP
| |
| +-System Name:                          AP_Cell_3
| +-SNMP IP Access List
|     Address   Mask           Interface
|     10.3.1.0  255.255.255.0  X
|     10.3.2.0  255.255.255.0  X
|
+-*Access Control
| |
| +-Setup Access Control
|     MAC Address        Comment
|     00:60:1D:04:2E:24  MN WaveLAN card
|     00:60:1D:04:2E:25  WC1 WaveLAN card
|     00:60:1D:04:2E:26  WC2 WaveLAN card
|     00:60:1D:04:32:96  WC3 WaveLAN card
|     00:60:1D:04:32:D6  tmp WaveLAN card
|
+-*Ethernet Interface
  |
  +-10 Mbit/s Full Duplex (Twisted Pair Port)  Yes
```

Glossary

IEEE 802.11

ad hoc network: A network composed solely of stations within mutual communication range of each other via the wireless medium. The term ad hoc is often used to refer to an independent basic service set.

AP (access point): Any entity that has station functionality and provides access to the distribution services, via the wireless medium for associated stations.

beacon: A periodic message sent by an AP containing synchronization and advertisement information.

BSS (basic service set): A set of stations controlled by a single coordination function.

BSSID (basic service set identifier): A network name for a basic service set, which normally corresponds to the station's medium access control address of its wireless LAN card.

dB (decibel): A logarithmic unit of intensity used to indicated power lost or gained between two signals.

dBm (decibels): A logarithmic unit describing decibels above or below 1 mW, synonymous to the gain or the loss in a signal. ($0\,\mathrm{dBm} = 10 * \log 1\,\mathrm{mW}$, $30\,\mathrm{dBm} = 10 * \log 1000\,\mathrm{mW}$)

DS (distribution system): A system used to interconnect a set of basic service sets and integrated LANs to create an extended service set.

DSM (distribution system medium): The medium or the set of media used by a distribution system for communications between access points of an extended service set.

DSS (distribution system service): The set of services provided by the distribution system that enable the medium access control to

transport its service data units between stations that are not in direct communication with each other over a single instance of the wireless medium.

ESS (extended service set): A set of one or more interconnected basic service sets and integrated LANs that appears as a single basic service set to the logical link control layer at any station associated with one of those basic service sets.

ESSID (extended service set identifier): A network name for an extended service set.

IBSS (independent basic service set): A basic service set that forms a self-contained network, and in which no access to a distribution system is available.

SNR (Signal-to-Noise Ratio): The difference in decibel between the received signal level and the noise level.

SS (station service): The set of services that support the transport of medium access control service data units between stations within a basic service set.

station: Any device that contains an IEEE 802.11 compliant medium access control and physical layer interface to the wireless medium.

wireless medium: The medium used to implement the transfer of protocol data units between peer physical layer entities of a wireless LAN.

IP and Mobile IP

agent advertisement: A router advertisement message with a special extension.

AR (access router): The last router between the network and the mobile node, i.e., the mobile node has link layer connectivity to the access router.

COA (care-of address): An IP address associated with a mobile node while visiting a foreign link.

CN (correspondent node): A peer node with which a mobile node is communicating.

FA (foreign agent): A router on a mobile node's visited foreign link which provides routing services to the mobile node while registered.

foreign link: Any link other than the mobile node's home link.

gratuitous (unsolicited) ARP: An ARP reply message (providing a mapping between the sender's IP address and link layer address) which is not prompted by any corresponding ARP request message.

HA (home agent): A router on a mobile node's home link with which the mobile node has registered its current care-of address.

home address: An IP address assigned to a mobile node within its home link.

home link: The link on which a mobile node's home subnet prefix is defined.

host: Any node that does not act as a router (i.e. forward packets).

MN (mobile node): A node that can change its point of attachment from one link to another, while still being reachable via its home address.

node: A network device that implements IP. It may act as a host or as a router.

RA (router advertisement): An ICMP router discovery message used to advertise the existence of neighboring routers to hosts.

Bibliography

[1] Agere Systems. *AP Manager*. Available online from `http://www.orinocowireless.com`.

[2] Benny Bing. *High-Speed Wireless ATM and LANs*. Artech House Publishers, 2000.

[3] Bob Braden et al. *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*. Request for Comments 2205, Network Working Group, September 1997. Available online from `http://www.faqs.org/rfcs/rfc2205.html`.

[4] Andrea De Carolis et al. *QoS-Aware handover for Mobile IP: Secondary Home Agent*. Internet-Draft, IETF Mobile IP Working Group, April 2001. Available online from `http://www.ietf.org/internet-drafts/draft-decarolis-qos handover-02.txt`.

[5] Stephen E. Deering and Robert M. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. Request for Comments 2460, Network Working Group, December 1998. Available online from `http://www.faqs.org/rfcs/rfc2460.html`.

[6] Gopal Dommety et al. *Fast Handovers for Mobile IPv6*. Internet-Draft, IETF Mobile IP Working Group, July 2001. Available online from `http://www.ietf.org/internet-drafts/draft-ietf-mobileip-fast-mipv6-02.txt`.

[7] Karim El Malki et al. *Low Latency Handoff in Mobile IPv4*. Internet-Draft, IETF Mobile IP Working Group, October 2001. Available online from `http://www.ietf.org/internet-drafts/draft-ietf-mobileip-lowlatency-handoffs-v4-02.txt`.

[8] ETSI. *HIgh PErformance Radio Local Area Network (HIPERLAN) Type 1*. ETSI Std EN 300 652, European Telecommunication Standards

Institute, July 1996. Available online from
http://pda.etsi.org/pda.

[9] Scott Fluhrer, Itsik Mantin, and Adi Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4.* Proceedings of the Eighth Workshop on Selected Areas in Cryptography, August 2001. Available online from http://www.crypto.com/papers/others/rc4_ksaproc.ps.

[10] David Gibson. *Orinoco.* Available online from
http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Orinoco.html.

[11] Dynamics Group. *Dynamics - HUT Mobile IP.* Available online from http://www.cs.hut.fi/Research/Dynamics.

[12] IETF SeaMoby Working Group. More information available online from http://www.ietf.org/html.charters/seamoby-charter.html.

[13] Stan Hanks et al. *Generic Routing Encapsulation (GRE).* Request for Comments 1701, Network Working Group, October 1994. Available online from
http://www.faqs.org/rfcs/rfc1701.html.

[14] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* IEEE Std 802.11-1999, Institute of Electrical and Electronics Engineers, August 1999. Available online from http://standards.ieee.org/getieee802/802.11.html.

[15] ISO/IEC. *Open System Interconnection – Basic Reference Model.* International Standard ISO/IEC 7498-1:1994(E), International Organization for Standardisation, November 1994. Available online from http://isotc.iso.ch/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm.

[16] David B. Johnson and Charles E. Perkins. *Mobility Support in IPv6.* Internet-Draft, IETF Mobile IP Working Group, July 2001. Available online from
http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-14.txt.

[17] Lucent Technologies. *... IEEE 802.11 channel selection guidelines.* WaveLAN Technical Bulletin 003/A, November 1998. Available online from http://www.novocomp.com/prod/wirl/WLAN/rWlanD.shtml.

[18] Lucent Technologies. *... roaming with WaveLAN/IEEE 802.11.* WaveLAN Technical Bulletin 021/A, December 1998. Available online from http://www.novocomp.com/prod/wirl/WLAN/rWlanD.shtml.

[19] Lucent Technologies. *... Planning Large Scale Installations.* WaveLAN Technical Bulletin 023/B, April 1999. Available online from `http://www.novocomp.com/prod/wirl/WLAN/rWlanD.shtml`.

[20] Lucent Technologies. *... security.* WaveLAN Technical Bulletin 002/A, September 1999. Available online from `http://www.novocomp.com/prod/wirl/WLAN/rWlanD.shtml`.

[21] Tom Z. Meinlschmidt. *WaveLAN Monitor.* Available online from `http://salome.datron.cz/~znouza/projects/wavelan/`.

[22] Charles E. Perkins. *IP Encapsulation within IP.* Request for Comments 2003, Network Working Group, October 1996. Available online from `http://www.faqs.org/rfcs/rfc2003.html`.

[23] Charles E. Perkins. *IP Mobility Support.* Request for Comments 2002, Network Working Group, October 1996. Available online from `http://www.faqs.org/rfcs/rfc2002.html`.

[24] Charles E. Perkins. *Minimal Encapsulation within IP.* Request for Comments 2004, Network Working Group, October 1996. Available online from `http://www.faqs.org/rfcs/rfc2004.html`.

[25] Charles E. Perkins and David B. Johnson. *Route Optimization in Mobile IP.* Internet-Draft, IETF Mobile IP Working Group, September 2001. Available online from `http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-11.txt`.

[26] Charles E. Perkins and Kuang-Yeh Wang. *Optimized Smooth Handoffs in Mobile IP.* Proceedings of the Fourth IEEE Symposium on Computers and Communications, July 1999. Available online from `http://citeseer.nj.nec.com/perkins99optimized.html`.

[27] James D. Solomon. *Mobile IP: The Internet Unplugged.* Prentice Hall PTR, 1998.

[28] Jean Tourrilhes. *Wireless Tools.* Available online from `http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html`.

[29] Attila Weyland. *Wireless LAN Monitor.* Available online from `http://www.iam.unibe.ch/~weyland/src/wlmon.tar.gz`.

[30] Attila Weyland. *Evaluation of Mobile IP implementations under Linux.* Project report, University of Berne, December 2000. Available online from `http://www.iam.unibe.ch/~rvs/publications/Mobile_IP.pdf`.

[31] Thomas Williams, Colin Kelley, et al. *Gnuplot*. Available online from `http://www.gnuplot.org`.

[32] Moustafa A. Youssef. *MWaveLan*. Available online from `http://www.cs.umd.edu/ moustafa/mwavelan/mwavelan.html`.