Mobility Support in IP Cellular Networks — A Multicast–Based Approach

vorgelegt von
Diplom-Ingenieur
Andreas Festag
aus Berlin

von der Fakultät IV - Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
– Dr.-Ing. –

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender:	Prof. Dr.-Ing. Dr. rer. nat. H. Boche
Berichter:	Prof. Dr.-Ing. A. Wolisz
Berichter:	Prof. Dr. G. Polyzos

Tag der wissenschaftlichen Aussprache: 5. Juni 2003

Berlin 2003

D 83

To my family.

Zusammenfassung

Heutige zellulare Kommunikationsnetzwerke bieten eine unterbrechungsfreie Mobilitätsunterstützung, basieren aber auf homogener Netzwerktechnologie und komplexer verbindungsorientierter Infrastruktur. Es ist zu erwarten, dass die Internet-Technologie einen Paradigmenwechsel bei zellularen Netzwerken herbeiführen wird. *Mobile IP* stellt die klassische Lösung für das Mobilitätsproblem in IP zellularen Netzwerken dar, hat aber eine Reihe von Nachteilen: das indirekte Routing und der Einfluss auf die Ende-zu-Ende Verzögerung, Probleme durch sogenannte *Ingress*-Filter bei Routern, sowie die ungenügende Qualität des Handover.

In dieser Dissertation wird der Ansatz verfolgt, das Mobilitätsproblem mit Unterstützung von Gruppenkommunikation (Multicast) zu lösen. Hierbei wird im Prinzip die Fähigkeit des Multicast zur Adressierung und zum Routing unabhängig vom Aufenthaltsort genutzt. Dadurch stellen sich aber eine Reihe von neuen Herausforderungen, unter anderem die Tatsache, daß Multicast nicht alle Funktionen bietet, die zur Mobilitätsunterstützung notwendig oder wünschenswert sind. Ebenso stellen sich Probleme von Multicast in nicht-mobilen Netzwerken, sowie durch die besonderen Anforderungen von Hostmobilität an den Multicast. Auf diesem Gebiet gibt es bereits mehrere interessante Vorschläge, denen unterschiedliche Motivation, sowie verschiedene Anforderungen und Annahmen über die Netzwerkarchitektur zugrunde liegen.

Es werden die Anforderungen an Multicast-basierte Mobilitätsunterstützung identifiziert, sowie Mobilitätsfunktionen und grundlegende Protokolloptionen ausgearbeitet. Diese drei Komponenten bilden ein Rahmenwerk für einen System- und Protokollentwurf für Multicast-basierte Mobilitätsunterstützung, genannt MOMBASA (**Mo**bility Support – A **M**ulticast-**Bas**ed **A**pproach). Dieses Rahmenwerk wird benutzt, um existierende Arbeiten zu beurteilen und dient gleichzeitig als Basis, um neue Ansätze zu kreieren bzw. existierende zu modifizieren. Vier Fallstudien, basierend auf unterschiedlichen Dienstmodellen für Multicast, werden von dem Rahmenwerk abgeleitet.

Zur Untersuchung der Fallstudien wird ein kombinierter Ansatz aus Messung, Simulation und Analyse angewendet. Für eine experimentelle Untersuchung wurde die *MOMBASA Software Environment* entwickelt, eine generische Softwareplattform für die Untersuchung von Multicast-basierter Mobilitätsunterstützung in IP-basierten Netzwerken. Die Softwareplattform bietet ein abstraktes Interface zum Multicast und ist daher auch zur zukünftigen Untersuchung von unterschiedlichen Typen von Multicast geeignet. Die *MOMBASA Software Umgebung* ist Teil der Umgebung zur Leistungsbewertung, die es gestattet, die Fallstudien in einer gemeinsamen Umgebung unter vergleichbaren experimentellen Bedingungen zu untersuchen.

Die Ergebnisse der Dissertation zeigen die prinzipielle Möglichkeit eines mobilen Kommunikationssystems mit Multicast-basierter Mobilitätsunterstützung ohne Einschränkungen von IP-Diensten. Potentielle Probleme (wie z.B. das Fehlen eines zuverlässigen Transportdienstes für Multicast) können vermieden werden. Die Dissertation beschreibt die Ergebnisse der Leistungsbewertung für Handover. Es werden Skalierbarkeitsaspekte untersucht, insbesondere die Signalisierungskosten in einem System mit Multicast-basierter Mobilitätsunterstützung ermittelt. Alle Ergebnisse werden mit dem Referenzfall Mobile IP und seiner hierarchischen Variante verglichen.

Abstract

Today's cellular communication networks offer seamless mobility support but are based on a homogeneous networking technology and a complex voice-oriented networking infrastructure. The Internet technology is expected to cause a paradigm shift in cellular communication networks. Mobile IP is the classical solution to support host mobility, but faces a number of disadvantages, including triangular routing and its effect on protocol overhead and end-to-end delays, router ingress filtering, and handover performance.

In the dissertation a different approach is pursued that solves the general mobility problem by means of group communication (multicast). In principle, it utilizes the capability of multicast for location-independent addressing and routing, but poses a number of challenges, including the fact that not all mobility functions are offered by the multicast, as well as the open problems of the multicast as it exists in today fixed networks, and problems that arise through the usage of multicast for mobility support, such as the scalability with the number of multicast groups. A few proposals in this area have already been made with different motivations, requirements, and assumptions about the networking architecture.

In this dissertation the requirements for multicast-based support of host mobility are identified, as well as mobility functions and basic protocol options elaborated. The three components create a framework for the system and protocol design of multicast-based mobility support that is termed MOMBASA (**Mo**bility Support – A **M**ulticast-**Bas**ed **A**pproach). The framework is used to judge existing research approaches and serves as a basis to design new schemes and modify existing ones. Four case studies are derived from the framework based on the *Any-Source Multicast*, the current multicast standard in the Internet, as well as alternative service models. For these case studies a set of protocols are designed that augments the multicast schemes by mobility functions.

The methodology of investigation is a combined approach of measurements, simulation, and analysis. For experimental investigation the *MOMBASA Software Environment* is developed – a generic software platform for experimentation with multicast-based mobility support in IP-based networks. The software environment offers an abstract interface to the multicast, and hence can be used for future investigations of different classes and types of multicast. The *MOMBASA Software Environment* is part of the evaluation environment that allows to investigate the selected case studies in a common experimental environment under comparable conditions.

The results of the dissertation show the feasibility of a mobile communication system with multicast-based mobility support providing the full spectrum of IP services. Potential problems of multicast-based mobility support (e.g. lack of a reliable transport service for multicast, and others) can be avoided. The dissertation presents results of the performance evaluation for handover. Scalability issues are addressed, in particular the signaling costs in a system with multicast-based mobility support determined. All results are compared with the reference case Mobile IP and its hierarchical variant.

Contents

List of Tables

List of Figures

1. Introduction

The recent years have seen a rapid development of mobile computing and communication. The technological progress was driven by advances in wireless and wireline transmission technology, cellular technology, communication protocols, micro-electronics and standardization efforts. Mobile service has evolved from a sparse coverage and heavy mobile devices – mainly for vehicles – to an almost ubiquitous coverage with very small-size devices affordable to users. While today's mobile systems are still being optimized for voice communication, they support an increasing variety of mobile data services at low data-rates.

The future of mobile communication is sometimes considered in the context of *Ubiquitous Computing*. This is a vision of a future world, which enhances computer use by providing many devices to anyone and making them effectively invisible to the user:

> *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."*
>
> "The Computer for the 21st Century", M. Weiser [163]

A vision like this makes great demands on mobile networks, and in this context, problems need to be solved before *Ubiquitous Computing* becomes a reality. Certainly, the next generation of mobile network will cope with some of these problems. For example, technologies such as GPRS and UMTS will offer a connection-less service in the near future and, therefore, introduce a paradigm shift from connection-oriented to connection-less communication in mobile networks. In order to shape future networks, it is essential to identify trends in the development of present-day mobile networks. By identifying the trends, the design of future mobile networks becomes clearer. In what follows, major trends will be highlighted.

New wireless technologies. A variety of new wireless technologies will replace or augment existing radio technology, such as IEEE WLAN [86, 87, 88], UTRAN based on WB-CDMA [41], or Bluetooth [71] and will be used instead or complementary to GSM and IS-95 radio technology. Each of these technologies will offer a different service in terms of bandwidth and (partly overlapping) spatial coverage. There is no wireless technology that provides all requirements all the time, and there is a tradeoff between coverage, data rates and costs. Hence, future mobile networks will not base on a single standardized wireless interface, but on a set of different technologies and standards.

High-speed core networks. Future core networks will provide very high bandwidth. In particular, optical fiber transmission offers abundant bandwidth with data rates beyond gigabit per second. This technology meets the requirement of a large bandwidth transport capability in the core network, which interconnects cellular access networks. In existing core networks optical technology is only utilized for point-to-point transmission and electrical processing is done at every node. Future photonic networks are expected to provide direct optical connections without electrical processing using wavelength routing.

Variety of communication devices. Future mobile networks will support a variety of communication and computing devices, that differ in their physical equipment. This equipment may include screens, video and sound support, input devices (touch screens, pointer, keyboards, voice recognition), data processing capabilities, storage and network devices. In particular it is expected that devices will be equipped with more than one network interface in parallel. With the progress of software radio technology wireless interfaces will be able to adapt to the current environment and switch between different modes if demanded or beneficial.

New communication services. Speech will continue to be the predominant source of traffic, but at a quality comparable to fixed networks. Mobile Internet access can be regarded as the basic data services for mobile users, which facilitates the use of popular applications well known from the wireline Internet access, such as email, web browsing, streaming audio and video, file transfer, network games, ICQ, remote execution of programs. Moreover, mobile communication paves the way for new services, such as E-shopping and location-based services.

IP-based network nodes and protocols. Future mobile networks will use the Internet model where Internet Protocol (IP) packets are used for both transport and signaling. IP-aware network nodes and devices can give better support to IP applications. They will reduce the cost of deployment, and in addition IP-style engineering is faster and cheaper, as the Internet development has proven. IP-based protocols facilitate a natural convergence of fixed and mobile networks. Finally, considering the wireless interface, an IP-based protocol enables the movement between access points and networks that use different wireless interfaces.

Protocol conversions. Although IP-based applications will dominate future traffic volume, existing standardized services (conventional voice, fax, old-style data applications) will still be supported by means of conversions. This includes application-level protocols with media conversions (e.g. fax-to-jpeg, email-to-voice, etc.). Also well-known standardized supplementary services, such as GSM call forwarding are expected to be re-implemented in IP-based applications. Such protocol conversions are also required since equipment often has limitations in processing capabilities, screen resolutions, etc. and not all applications can be used in all end systems.

Future mobile networks will offer services where users can move freely almost anywhere and communicate with any one, any time, and in any form using the best service available. They will support different types of mobility: In a scenario with nomadic wireless access the user roams freely and the mobile device switches between access points only between two consecutive communication sessions. In a scenario with true mobility dynamic changes of the supporting access point during a session – usually referred to as handover – are expected to appear, possibly even several times during a single session. The grade of service continuity in spite of handover is one of the essential quality features. Continuity of service might be expressed in terms of no information loss during the handover, sometimes even so-called seamless handover, i.e. handover not observable by the user at all. In order to provide seamless handover across possibly heterogeneous networks it is required that the networks interact and co-operate to offer the best service available. The latter scenario lies in the focus of this thesis.

1.1. Mobile Communication

Wired and wireless communication networks differ in an essential property: In wired communication networks, the supported data rate can be increased to a nearly unlimited degree in exchange for added investment in equipment. In contrast, the overall data rate in wireless communication networks is limited due to spectrum scarcity. In order to make efficient use of the available spectrum, present-day wireless communication networks *reuse channels*. This channel reuse exploits the physical phenomenon of wireless transmission, i.e. wireless signals are attenuated after a certain distance and do not interfere. In order to utilize the channel reuse in communication networks, the coverage of a wireless network is divided into smaller areas called *cells* (Fig. 1.1). The available spectrum is split into (logical) channels. These channels are distributed among the cells according to a certain reuse pattern. In addition, the power levels used within a single cell are limited in order to reduce interference between the cells. In the early wireless networks, the *seven-cell-reuse-pattern* was used, which was a result of the distance required between cells using the same logical channel. By channel reuse, more users can be accommodated in a wireless network as if the channel is used a number of times in the system.

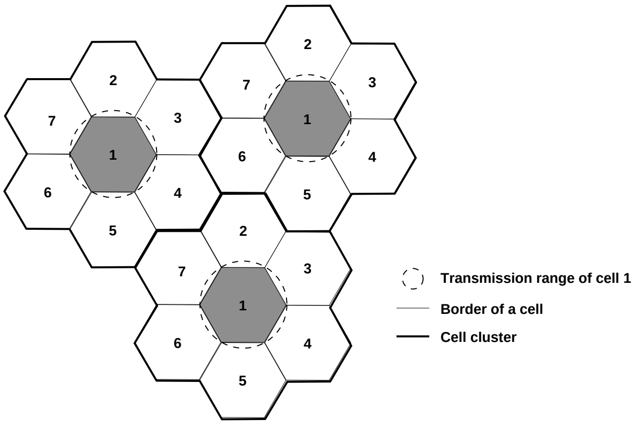


Figure 1.1.: Cellular structure of a wireless network

Cellular networks exploiting channel reuse requires a dedicated access point – a dedicated network node that provides service in the spatial coverage of a cell. The access points are interconnected by a – usually fixed – network infrastructure.

The cellular principle gives rise to mobility-related phenomena which are not present in non-cellular networks. In order to establish communication sessions with a mobile user, the communication network needs to determine the mobile user's location and the actual communication path to the user. This is a similar functionality in relation to fixed networks, but the difference is that in cellular networks the mobile user's current location can change. Therefore, a cellular communication network maintains location information of users in a – centralized or distributed – database. A mobile user frequently updates the network with its actual location information. Without the location database in the network, a mobile user would need to be located by means of searching the whole service area of the communication network.

Another mobility-related phenomenon is caused by the migration of a mobile user from one cell to another while a communication session is ongoing. This process is referred to as *handoff* or *handover*, and may cause disturbances, or even break off communication sessions.

The growing demand for higher data rates results in very small cells – called micro cells, pico cells and even nano cells with diameters of several meters. This trend clearly follows from the use of higher radio frequencies: the higher the radio frequency the higher the attenuation and the worse the wall penetration. Smaller cells with a high grade of user mobility (i.e. speed) result in very frequent handover which may disturb the communication service remarkably. To supply the environment efficiently, cellular networks consist of cells with different spatial coverage (forming a hierarchy of cellular layers). Pico-cells will be provided in communication *hot spots*, whereas macro-cells supply a basic communication service. Frequent handover with stringent requirements on the communication quality as well as handover between cells of different cellular layers require sophisticated mechanisms for mobility support. These mechanisms will be dealt with in this thesis.

1.2. Thesis Formulation

Today's cellular communication networks offer seamless mobility support but are based on a homogeneous networking technology and a complex voice-oriented networking infrastructure. The Internet architecture, protocols, and applications provide flexible services with heterogeneous networking technology at prospectively lower costs. The Internet technology is expected to cause a paradigm shift in cellular communication networks: In an all-IP cellular network wireless end systems represent IP hosts and the network nodes of the cellular backbone are based on IP routers of an access network interconnected to the global Internet.

A general problem, however, needs to be solved: An IP address reflects a host identifier as well as the host's current network point of attachment as the location. This IP address is used to establish a session between hosts, whereas sockets at an protocol-independent interface are used to access lower protocol-dependent layers. A *mobile* host might change its current network point of attachment so that the network part of the mobile host's IP address does no longer match the IP network address of the new location. The assignment of a new IP address – which is topologically correct – enforces the closure and re-opening of existing sessions and their corresponding sockets. In fact, sockets are bound to source and destination addresses. Hence, the re-establishment pertains to the mobile as well as to a correspondent host communicating with the mobile host and disrupts the communication. Even frequent changes of the network point of attachment considerably sustain the communication quality.

A number of solutions for the general mobility problem already exists. They can be divided into three main categories: *Indirect addressing and address translation* (e.g. Mobile IP [96, 129], RAT [147]) assign two IP unicast addresses to a mobile host: A permanent address and a temporary address. Packets destined to the mobile host are routed indirectly via the mobile host's home network where a home agent translates the IP address in the packet to the mobile host's temporary IP address. The second category is *Host-based routing* (e.g. Cellular IP [27], HAWAII [136]) where an IP address is considered as a unique host identifier without a network part and routing is performed by means of the host identifiers. Since the IP address does not reflect the location, it is not necessary to assign a new IP address during a handover. For routing of packets the network nodes have per-host-entries that are created and released according to the mobile host's movement. *Application proxies* (e.g. MPA [161], ICEBERG [105], Extended SIP [162]), the third category, introduces a new user-level addressing concept and principally maps the user address to the temporary IP address of the mobile host. When a mobile host changes its IP address due to mobility, the user address is re-mapped to the mobile host new IP address.

In this thesis, however, a different approach is pursued. The general mobility problem – as described above – is solved by multicast. The main idea of multicast-based mobility support is to utilize location-independent addressing and routing to support host mobility. In principle, each mobile host is assigned a multicast group address – a special-purpose address that does not contain a network part and, therefore, is independent of the location. The mobile host subscribes to the multicast group through its current access point to the network. Handover is performed by multicast operations, namely subscribe/un-subscribe to/from a multicast group. Data packets are distributed via a multicast tree with branches reaching the current locations of the mobile host on its movement. The branches of the multicast tree can grow and shrink, and hence, follow the mobile host's location. In particular, the branches can be simultaneously set up to multiple locations, including the current as well as the expected locations of the mobile host. In comparison to the classical solution for IP mobility support, Mobile IP, a multicast approach has the following advantages: *First*, re-routing for handover is done in a network node where the paths to the old and from the new access point diverge (and not in a software agent in the mobile host's home network as in the Mobile IP approach). *Second*, a handover-specific signaling and infrastructure is in principle not required, instead multicast is reused for mobility purposes. And *third*, multicast offers inherent mechanisms to minimize the service interruption caused by a handover between access points.

The utilization of multicast for mobility support poses many challenges. First of all, multicast does not offer all functionalities that are required for mobility support or useful for mobility-related performance. Another set of problems arises from the design of present-day IP multicast – these problems exist independently of its potential use for mobility purposes. Other challenges are caused by the specific requirements of mobility support on multicast. Highly dynamic join and leave operations represent an example for such a requirement.

It has already been recognized that multicast has a number of attractive features for the support of host mobility and this idea has been addressed by a few research studies. These studies have certain requirements and make particular assumptions about the network architecture and protocols, in particular about the used multicast type. Instead of developing a single solution as in the existing approaches, in this thesis a framework for the system and protocol design of multicast-based mobility support is developed that is not limited to the classical IP multicast service model. This framework is termed Mobility Support - A Multicast Based Approach (MOMBASA). The components of the framework are requirements, protocol options and mobility functions. The framework create a basis to judge existing approaches and to derive certain case studies. While these case studies have similarities in basic protocol options, such as location of the multicast end point, they differ in others, such as the provided the multicast service model. Consequently, the case studies provide different options of mobility functions by optimally utilizing the specific features of their multicast.

In this thesis, four case studies are defined that attempt to meet the above mentioned challenges of multicast-based mobility. These case studies represent extensions of existing approaches or new schemes. It is common to all case studies that the multicast schemes itself keep unmodified and are not adapted for mobility purposes. Instead the basic multicast functions (including group creation and release, subscription, un-subscription, data transport) are augmented by a set of mobility functions, such as handover initiation and others.

The methodology of investigation is a combined approach of experimentation, simulation, and analysis. For experimental investigation, the *MOMBASA Software Environment*, a generic software platform for experimentation with multicast-based mobility support in IP-based networks is developed. Basically, it is composed of software components for mobile hosts, mobility-enabling proxies and gateways. The *MOMBASA Software Environment* can be regarded as a subset of functionality of the general approach *MOMBASA* that are implemented as prototypes. Moreover, the software environment offers an abstract interface to the multicast, and hence can be used for future investigations of different classes and types of multicast. In this thesis the *MOMBASA Software Environment* is used to evaluate the performance of the selected case studies in a common experimental environment.

1.3. Thesis Outline

The thesis is organized as follows:

In the second chapter of the thesis the concept of mobility support in communication networks is introduced. After the definition of related terminology, the architecture of IP networks, in particular IP-based wireless networks are detailed. Then requirements on the design of schemes for mobility support are described. Based on this requirement analysis, existing approaches for mobility support in wireless IP-based networks are reviewed.

Chapter 3 explains the fundamentals of multicast, including link-layer multicast, network-layer multicast, and application-layer multicast, and analyzes existing multicast protocols in connection-oriented and connection-less networks.

The following chapter 4 describes a general framework for multicast-based mobility support by analyzing requirements, protocol options and functionalities. Existing approaches to multicast-based mobility are reviewed, and it is shown how these approaches can be captured within the framework. Then, the framework is utilized to derive four case studies for multicast-based mobility support and the reasons for the selections are stated. These case studies are investigated in detail in the following chapters. The four case studies represent new approaches to multicast-based mobility support and extend existing schemes, respectively.

The following chapters focus on the selected case studies: Chapter 5 describes the methodology of investigation. It critically discusses the selection of an evaluation technique, describes the assumed network model for the experimental investigations, simulation, and analysis and introduces the evaluation criteria. Chapter 6 presents the design of the protocols that has been developed. Chapter 7 describes the software platform. Chapter 8 describes the measurement environment, presents the evaluation results of the particular case study, and compares the results of the case study with the reference case basic and hierarchical Mobile IP.

2. Mobility Support in Communication Networks

This chapter gives an overview of mobility support in communication networks with emphasis on IP networks. Therefore, terms related to mobility support are exactly defined and the architecture of IP networks is introduced. Extensive studies of mobility support in IP-based networks have already been carried out. As it will shown, some of the approaches are based on the same principles. The approaches are reviewed, categorized and compared. Multicast-based mobility support can be regarded as a different class of approaches. Therefore, the existing multicast-based approaches to mobility support will be reviewed separately in the next chapter – after the fundamentals and protocols of multicast have been explained.

This chapter is organized as follows: First, a general overview of mobility support in communication networks is presented. Then, the architecture of IP-based networks is detailed. This includes addressing and routing mechanisms that lead directly to the fundamental mobility problem in IP. Then, the requirements for the design of mobility schemes are elaborated and Mobile IP, classical solution for mobility support, introduced. Based on a discussion of weaknesses of Mobile IP, existing alternative approaches to unicast-based mobility support are reviewed.

2.1. Terminology

A **communication network** carries information between users. Users are equipped with communication devices and data is exchanged between devices by means of a communication network. A communication network offers either a **connection-oriented** or a **connection-less** service to applications. With a connection-oriented service applications executed in the devices exchange control messages to establish connections before sending messages with user data. With a connection-less service no handshake procedure prior to transmission of messages is needed. Applications simply send the messages. In the past a communication device was typically fixed to a single location. With the technological progress a formerly fixed telephone became a tether-less cellular phone and a computer became a portable laptop or even small-sized palm-top. Wireless communication allows an information exchange to and from a wireless communication device. A **wireless network** provides the infrastructure for wireless communication.

In oder to make efficient use of the available spectrum, today's wireless networks partition the available spectrum into channels and the spatial coverage of a network into smaller smaller areas termed *cells*. A channel represents a physical resource, such as a frequency slice, a set of time slots, or assigned codes. The type of the physical resource depends on the access technology. The channels are assigned to the cells applying a certain **reuse pattern**, in which the assignment scheme can be fixed (fixed channel assignment scheme) or dynamic. With the latter dynamic channel assignment scheme, the association between cell and channel may change e.g. due to changing traffic conditions. The exact size of a cell is defined by the signal-to-interference ratio and the boundary is usually fixed to a signal-to-interference ratio of 3 dB. Clearly, the size and shape of a cell depend on a number of parameters, such as frequency, transmission power and receiver sensitivity, environmental attenuation due to obstacles and walls, antenna directivity, noise, adjacent- and co-channel interference, and others. However, it is important to note that wireless cells may overlap or not, in the latter case creating a gap in service continuity.

More general, a **wireless cell** can be defined as the portion of the service area of a wireless network. Wireless networks that make use of the channel reuse concept require an **Access Point (AP)**. An access point is a dedicated node or physical component that provides a communication service within the spatial coverage of a wireless cell.

An access point connects a wireless device to wired **fixed networks** and to other wireless devices. The fixed network can be the Internet, the Public Switched Telephone Network (PSTN) or another type of network. The wireless interconnection between the mobile device and access point is termed **wireless link** and represents a logical connection. When access points of a wireless network use a single wireless technology the network is termed homogeneous, otherwise heterogeneous. In large communication networks, access points are combined to an **access network**. This is a fixed network under the control of a single authority. It interconnects the access points with a global network via a **gateway**.

A wireless device that moves through the coverage of a wireless network is usually named a **mobile terminal** or **mobile host (MH)**. When a mobile terminal moves out of the range of an access point and enters the range of a new access point a **handover**[1] occurs. A handover is a process that is executed when a mobile host migrates from one access point to another while communicating. This process transfers the responsibility for a mobile terminal from one access point to another. A handover includes a number of operations for handover detection, initiation and execution. Handover and other operations incorporate the exchange of messages between the mobile host and the network nodes and between network nodes termed **signaling**. **Roaming** is usually referred to as using a mobile host while away from the home network.

A mobile terminal usually registers on each handover with its actual access point. By means of registrations the network tracks the current location of a mobile terminal. Instead of tracking, a mobile terminal can be searched within the spatial coverage of the cellular network. The process of locating a mobile terminal within a geographical region is referred to as **paging**. Paging allows the mobile host to update the network less frequently and provides the network only with approximate location information.

Assuming that a communication network offers a certain service and communication sessions – terminal or network initiated – are established, then the user with the terminal may move within the spatial coverage of the service area. At least two basic scenarios for wireless access can be identified [170]:

In the first scenario – which is referred to as **nomadic wireless access** – the terminal is expected to be moved over distances essentially exceeding the transmission range of a single access point. It is assumed that a terminal may switch between the access points only between two consecutive sessions. This movement usually takes times which are relatively long compared to session duration. Typically, no hints can be used in which location – close to whichever access point – the terminal might appear after movement.

In the second basic scenario, which is referred to as **true mobile access**, the terminal moves freely in the service area of the network from one cell to another and dynamically changes the supporting access point during a session. As defined above, this process is referred to as handover and is expected to appear possibly several times during a single session. In this scenario, the grade of service continuity, in spite of handover, is one of the essential quality features of this scenario. The handover may result in a loss of communication which may not be noticeable in voice communication

[1] The terms handover and handoff are considered to be interchangeable.

but can result in loss of data for other applications.

Handover in particular communication networks differs greatly. In order to generalize handover procedures, handover can be classified with respect to the following criteria:

- the number of access points involved,
- the wireless link used for handover operation,
- the initiation of handover,
- the change of access technology caused by handover in heterogeneous networks,
- the topology of the interconnection network,
- the state of the terminal,
- the continuity of service,

Within these categories the following handover types can be defined:

- Criterion: Number of access points involved

Hard handover With hard handover the terminal has connectivity to a single access point, either the old or the new one in any point of time. Typically, TDMA-based wireless technologies, such as IEEE 802.11 employ hard handover. The control of hard handover is more simple since there is no ambiguity over which access point the mobile terminal shall communicate.

Soft handover With soft handover the terminal has connectivity to more than one access point simultaneously. It requires that wireless cells overlap. Certain access technologies offer soft handover functionality inherently. For example, in Wideband Code Division Multiple Access (WB-CDMA) [122] the neighboring cell frequencies are the same as in the current cell (frequency reuse of 1) and spreading codes are used to identify logical channels in a cell. Since a terminal is able to receive multiple logical channels simultaneously, a terminal can be connected to two or more access points. This facilitates the deferment of the point of time for the handover decision. Typically, a terminal switches to a *soft handover state* if it has connectivity to more than one access points. If the terminal is not in this state then the transmission power is controlled according to the cell which the terminal receives with the highest signal strength. With other access technologies, such as TDMA, soft handover can be realized at the expense of additional hardware, such as duplicated transmitters and receivers. The advantage of soft handover is the shorter service interruption caused by handover. An disadvantage is the duplication of data during the soft handover phase that may degrade the total system throughput. An additional handover type – the *softer* handover – is sometimes referred to as a handover between sectors of the same cell.

Predictive handover With predictive handover a set of access points may receive data for a mobile terminal in advance of handover. The current access point in the set is usually referred to as **active** and forwards the data to the mobile host, the other access points are **passive** and buffer the data. The buffered data are forwarded when the mobile terminal registers.

- Criterion: Wireless link used for handover operation

  Backward handover Backward handover uses the current access point to request a handover to a new access point. It allows the terminal to execute the handover procedure while the terminal still has connectivity. When the procedure is completed the current access point triggers the terminal to switch to the new access point by re-establishing the radio link. It is however assumed that the handover can be predicted.

  Forward handover A forward handover uses the new access point for handover signaling operations. Usually, forward handover is used when the mobile host has lost connectivity to the old access point.

- Criterion: Initiation of handover

  Terminal-initiated handover In terminal-initiated handover the terminal manages the handover process, i.e. decides both the time when to handover as well as the target access point. Usually, the handover is triggered when the signal strength of a neighboring cell exceeds the signal strength of the current cell by a given threshold.

  Network-initiated handover In network-initiated handover the network manages the handover process. It is assumed that the network is able to determine the target access point (e.g. by determining the location of the terminal using GPS or movement prediction, etc.).

  Network-initiated, terminal-assisted handover In this handover type the network initiates the handover based on information sent by the terminal. For example, the terminal may frequently send measurement reports with certain measurement values to the network and the network decides both the time when to handover as well as the target access point.

- Criterion: Change of access technology caused by handover in heterogeneous networks

  Intra-technology handover Intra-technology is a handover between access points using the same wireless technology. Hence, the network interface of the mobile host is usually not changed. A typical example is a handover between two access points with IEEE 802.11 technology.

  Inter-technology handover Inter-technology handover is a handover between access points using a different wireless technology. A typical example is a handover from a GPRS access point to an access with IEEE 802.11 technology. A handover from a smaller cell to a larger cell is often made without simultaneous connectivity to both cells since, in this case, the user typically leaves the spatial coverage of the smaller cell suddenly. Thus, a handover from a smaller to a larger cell is usually a hard handover, whereas during a handover from a larger to a smaller cell the mobile host is often connected to access points of the higher and lower layers simultaneously (soft handover).

- Criterion: Topology of the interconnection network

  Local handover In a local handover the terminal moves to a new cell that belongs to a network of the same administrative domain (e.g. service provider). This is sometimes referred to as **micro mobility**.

  Global handover In a global handover the terminal moves to a new cell that belongs to a network of a different administrative domain. **Macro mobility** is used as a synonym in contrast to micro mobility.

- Criterion: State of the terminal

Active handover Active handover is a handover of an active terminal, i.e. a communication session is ongoing.

Idle handover Idle handover is a kind of handover that is made when the terminal is in idle mode, i.e. it does not have an ongoing communication session. Idle handover presumes that the system distinguishes between idle and active hosts. Idle handover typically includes fewer operations than active handover. For example, with idle handover the mobile re-registers less often and fewer signaling operations are needed.

- Criterion: Continuity of service

Seamless handover With seamless handover the handover is un-noticeable to the user, i.e. the service interruption is not observable. Obviously this notion can only be expressed in terms of the application requirements.

Lossless handover With lossless handover no information loss caused by handover occurs. Information transport can be considered as reliable, even in the presence of handover. Often, a long gap in communication also results in high losses, and vice versa. Nevertheless, lossless handover is not necessarily the same as seamless handover. For example, lost information can be retransmitted and then, the non-seamless handover is lossless.

The defined terms will be used in the following chapters of the thesis to describe the developed mobility approach.

2.2. Architecture of IP-Based Networks

In general, an IP-based network consists of a number of interconnected components as shown in Fig. 2.1. An **internet** is a collection of interconnected **networks** that can be further sub-divided into **subnetworks** (subnets). Each **network** owns an identifying **network address** which differentiates it from other networks.

A network in turn is a collection of interconnected **hosts** . Each host carries an address which is unique within the network, more precisely, the interface in a host is identified by a unique address. The combination of network address and host address uniquely identifies the host within the extent of the internet. Hosts are assumed to be static and the unique identifier is often referred to as a permanent address [73].

Multiple networks or subnetworks are interconnected by special–purpose boxes, called **routers**. A router has multiple interfaces, each is identified by an IP address unique in each of the connected networks. A router can be attached to very different types of subnets, such as Ethernet, token ring, and point-to-point links. To enable routers to work correctly, the assignment of subnet addresses is managed by a central authority that does not permit duplicate addresses. In IP-based networks data units traversing the internet are called **datagrams** or **packets**. They carry source and destination **IP address** in their header. Routers examine the destination subnet address of packets arriving at their inputs to determine which output to use in order to route packets toward their destinations. Hence, the main functionality of IP routers is the forwarding of packets on a route through the network. This is referred to as connection-less transport of packets. As a connection-less protocol IP does not guarantee **in-order-delivery** of packets. That is, the sequence of packets as generated by a source does not have to be preserved when the packets are delivered to the destination. Preserving the sequence is left to higher layer protocols, such as the transport protocol **Transmission Control**

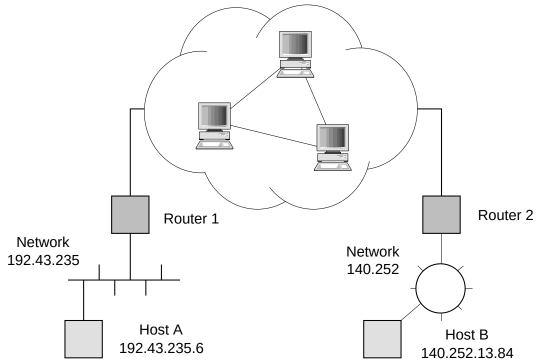


Figure 2.1.: General architecture of an IP network

Protocol (TCP) [42]. TCP preserves the sequence by offering a connection-oriented service. The **User Datagram Protocol (UDP)** [132] is a connection-less transport protocol without reliability as TCP.

In principle, the internet protocol works independently of the attached technology. From the router's perspective a link can be regarded as a transparent data pipe carrying IP packets. Even a path between two routers with a number of intermediate network nodes (e.g. switches) that transport packets transparently can be considered as a single logical link.

In IP version 4 an IP address consists of a 32 bit integer. Four address formats – termed address classes – are defined to allow for different sizes of networks to which a host is attached. The three primary classes A, B and C have three subfields. The first subfield identifies the address class, the other subfield specifies a **network identifier (net-id)** and a **host identifier (host-id)**. The fourth address class D is reserved for multicast. The following figures show the different address classes A, B, C, and D. Class D addresses are of particular importance for multicast-based mobility support. A class D address consists of a 4 bit identifier of the address class and a 28 bit host-id. It does not include a net-id. As an example, the network addresses 192.43.235 and 140.252 in Fig. 2.1 represent a class C and class B network, respectively.

- Class A

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|0|   net-id    |                   host-id                     |
```

- Class B

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|1|0|          net-id           |           host-id             |
```

- Class C

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|1|1|0|                  net-id                 |    host-id    |
```

- Class D

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|1|1|1|0|                        host-id                        |
```

The host-id portion of the IP address can further be subdivided into a **subnetwork identifier (subnet-id)** and a **host-id** [111]. This figure shows an example for a class B network address that is divided into a 8 bit subnet-id and a 8 bit host-id:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|1|0|          net-id           |  subnet-id    |    host-id    |
```

This sub-netting allows 254 subnets with 254 hosts per subnet. The number of bits allocated to the subnet-id is not fixed and committed to the local administration of the network.

Classless Inter Domain Routing (CIDR) [64, 138, 155] facilitates to allocate multiple IP addresses in a way that allows to summarize these IP addresses into a smaller number of routing table entries. The technique was motivated by to the shortage of unallocated class B addresses of IP version 4. In the past network operators have acquired multiple class C network identifiers instead of a single one for a class B network. Although this method solves the problem of scarce class B network identifiers, it introduces the problem that every class C network creates a routing table entry and results in greatly enlarged IP routing tables. CIDR allows the network operator to create a network without being restricted to the IP address classes with less routing table entries.

An IP packet carries a number of subfields, including source and destination address. The IP version 4 address format has placed limitations on the growth of the Internet. IP version 6 overcomes this limitation by increasing the size of the network addresses which are 128 bit long.

The internet protocol provides a number of core functionalities, including

- Fragmentation and reassembly of messages for transfer of packets across subnetworks which support smaller packet sizes than the user data of packets,
- Routing of packets through the network where each source must know the location of the local router directly attached to the same network/subnetwork,
- Error reporting to the source when packets are discarded by routers or some other reporting functions.

The global *Internet* can be regarded as a collection of separately managed internets with a **core network** (Fig. 2.2). The internets are termed **Autonomous System (AS)** and have their own internal routing algorithms and management authority. In order to discriminate between the gateways used within an autonomous system and those used to connect an autonomous network, the terms **interior gateway** and **exterior gateway** are used. The corresponding routing protocols are the **Interior Gateway Protocol (IGP)** and the **Exterior Gateway Protocol (EGP)** [139].

A number of companion protocols has been designed for use in IP-based networks forming the TCP/IP protocol suite or protocol stack. These protocols are modeled in layers. A comparison between the TCP/IP protocol suite and the ISO OSI reference model is shown in Fig. 2.3. In fact, the TCP/IP standards define many distinct communication protocols which have been evolved over 25 years.

A **wireless IP-based network** (Fig. 2.4) is a network with hosts that are connected by means of a wireless links and with components making use of the TCP/IP protocol suite. It is expected that in today's wireless networks more and more components will be replaced by IP-capable components. The final stage of this evolution is referred to as an **all-IP wireless network**. In an all-IP wireless network all components are replaced by IP networking equipment. Mobile hosts as well as the components in the fixed network carry IP addresses and execute applications that make use of TCP/IP protocols. Access points process IP packets and can be regarded as special-purpose IP routers. The access points are interconnected among themselves by a fixed network. This fixed network may include also routers forming a network. This network can be interconnected to the public Internet via a special-purpose router termed **gateway**. Very large wireless networks with many access networks attaching the public Internet via a single or multiple gateways are referred to as **wireless access networks**. The topology of a wireless network creates a hierarchical structure that consists of wireless hosts at the lowest hierarchical level, access points, and the gateway at the highest hierarchical level. In addition to this hierarchical topology of the access network the usage of heterogeneous wireless technologies in IP-based wireless networks results also in a spatial hierarchy

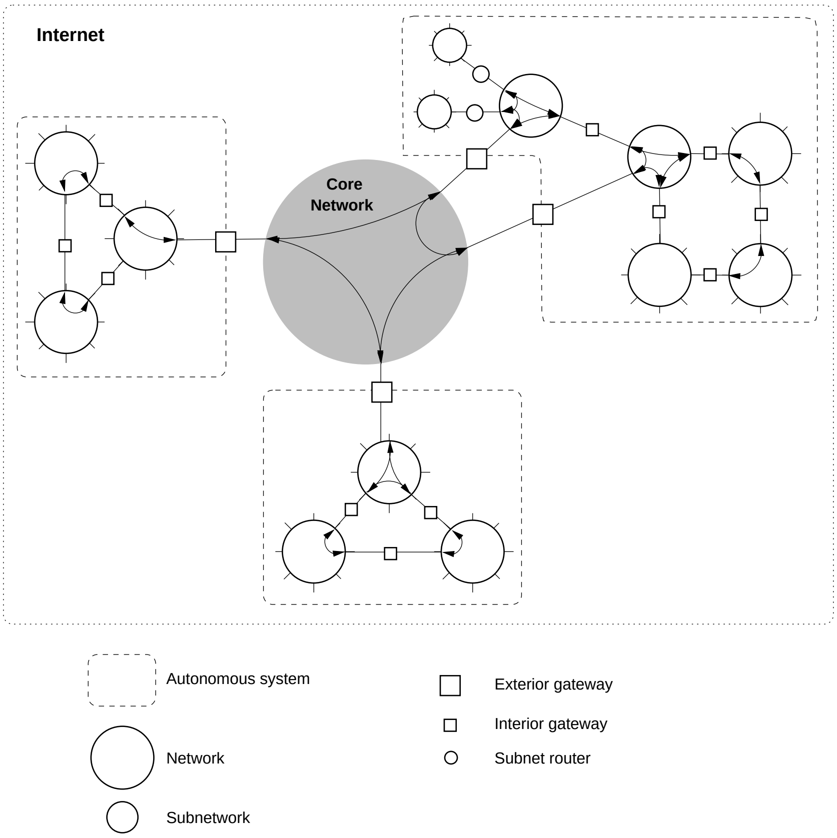


Figure 2.2.: Simplified architecture of the Internet composed of Autonomous Systems (AS) [73]

of wireless cells. This hierarchical structure is shown in Fig. 2.4 where small cells are located within the coverage of larger cells. Cells of common size and technology create a joint layer — the large cells can be regarded to be at the hierarchically higher layer and the smaller cells at the lower layer. Applying this model of a hierarchical wireless network an intra- and inter-technology handover type as described in Sect. 2.1 can be defined as horizontal and vertical handover. Horizontal handover can be considered as a transition of a mobile host between cells of the same hierarchy level, and vertical handover between cells of different hierarchy level.

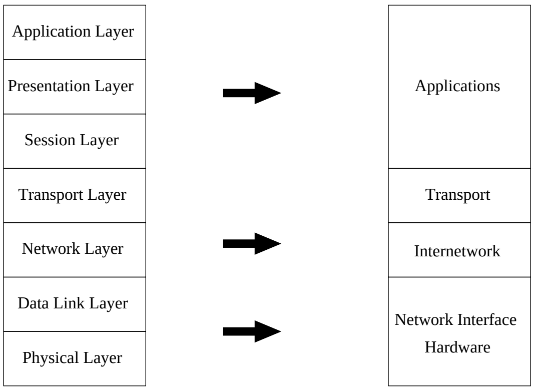


Figure 2.3.: TCP/IP protocol suite in comparison to the ISO OSI reference model

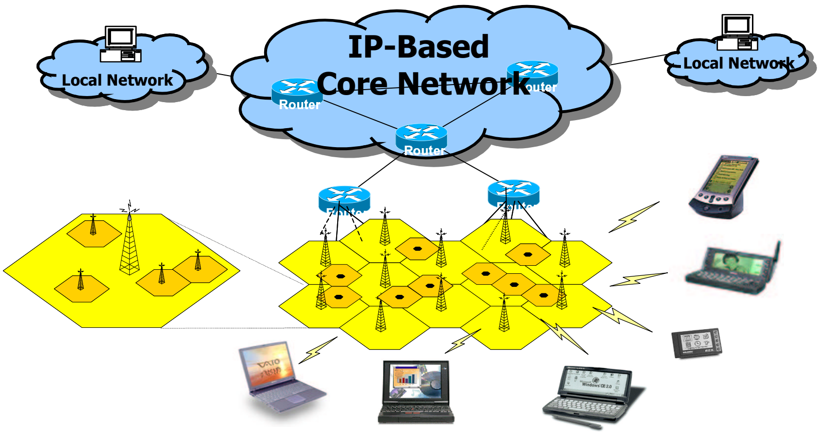


Figure 2.4.: Architecture of an IP-based wireless network

The usage of TCP/IP protocols in wireless networks implies many challenges. Many of them are related to mechanisms for wireless transmission, such as error control, flow control and congestion control. The support of host mobility is another important issue and will be examined within this thesis.

2.3. The General Mobility Problem in IP Networks

Originally, IP networks have been designed under the assumption that hosts are stationary. This assumption implies that the IP address does not change and a host is reachable from other hosts by an IP address that does not change. Data are carried by means of IP packets which contain source and destination addresses. Internet routers inspect the destination address contained in an IP packet. They make a forwarding decision based on the network part of the IP destination address and forward packets to the determined next hop. Consequently, this addressing scheme puts restrictions on the address usage. In particular, an IP address can only be used within the network of its definition. If a mobile host moves to a new network, the old IP address becomes topologically incorrect. Therefore, a new – topologically correct – IP address must be assigned to a mobile host.

In the TCP/IP protocol suite applications access communication services through a *socket layer* – a protocol-independent interface to the protocol-dependent below. When an application establishes a session between two host, it uses the IP address of the application‘s source node and the application‘s sink node comprised of the host-id and net-id and the IP address is interpreted as a host identifier. When a mobile host moves to a new network then the network part of the mobile host’s IP address does no longer match the IP network address of the new point of attachment. The same problem occurs if the network is divided into subnetworks: When a mobile host moves to a new subnetwork the subnet-id becomes incorrect. The assignment of a new IP address – which is topologically correct – enforces the closure and re-opening of existing communication sockets. In fact, sockets are bound to source and destination addresses. Hence, the re-establishment pertains to the mobile as well as to a correspondent host communicating with the mobile host and disrupts communication service.

This dichotomy – an IP address represents both host identification and location – is the fundamental mobility problem in IP-based networks. This problem needs to be overcome by mobility concepts.

2.4. Requirements for the Design of Schemes for Mobility Support

A general concern in wireless networks is the communication quality. The today’s cellular networks were mainly designed for voice applications. The requirements of these applications are low end-to-end delay and small jitter at a fixed data rate. In future IP-based wireless networks a diversity of applications with different application requirements are expected. A network that would meet the most stringent requirements for all applications – if possible – would inefficiently use resources. Therefore, applications used in wireless IP-based networks are classified into several categories with respect to their requirements for the service quality.

In principal, not all applications used in a wire-line environment work properly in a mobile environment. Therefore, some applications will be adapted to the limitations in a wireless environment (mobile host with small processing power and energy, limited bandwidth, etc.) and will have less stringent application requirements than in wire-line networks. Other applications can be kept unmodified, but should work with as little impairment as possible. Additionally, the mobility of hosts facilitates new applications (e.g. location-based services) and enable requirements for applications that are not known from non-mobile networks.

Another concern in wireless networks is scalability: It is expected that next generation wireless IP-based networks must support a very high number of mobile hosts, at least as many as the number of subscribers in today’s GSM networks. Therefore, any scheme for mobility support must be scalable with the number of mobile hosts and should minimize the **costs** for mobility support. Minimizing the impairment of application performance due to mobility, as well as the costs of mobility support are antagonistic requirements. As an example, a scheme that facilitates seamless handover for any application may incur a high signaling overhead which limits its scalability.

Key requirements of applications can be expressed in terms of Quality of Service (QoS) parameters

- delay and jitter,
- reliability, and
- bandwidth,

whereas the three parameters depend from each other.

Delay refers to the duration of time it takes to transmit a packet from the source to the destination. The delay includes the duration of time for packetization, physical transmission, queuing, and synchronization (e.g. waiting for corresponding samples from other data flows). The variation in delay is termed jitter. Jitter can be smoothed by means of packet buffering at the expense of a higher delay.

Reliability describes the requirement of the application to tolerate packet loss. Typically, packet loss is caused by congestion in the network. In wireless networks packet loss also occur due to an error-prone wireless channel. Error control, i.e. retransmission of packets or Forward Error Correction (FEC), improves the reliability at the expense of the delay and bandwidth.

Bandwidth expresses the data transmission capability of the network. On the one hand, the overall network bandwidth must meet the sum of the applications bandwidth requirements. On the other hand, it must be ensured that each application gets a fair share of the overall bandwidth.

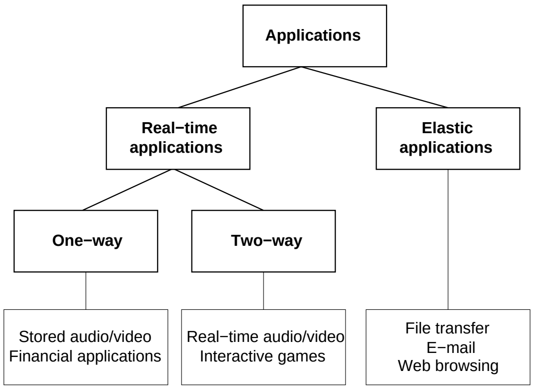


Figure 2.5.: Classification of IP applications with respect to their requirements

In order to classify IP applications with respect to their requirements it is common to distinguish applications by means of their requirements for delay (real-time and delay-insensitive) and data rate (independent data-rate and elastic): Typically, applications can be categorized into **real-time applications with independent data rate** (short real-time applications) and **elastic, delay-insensitive applications** (short elastic applications). A real-time IP application is based on packetization of a source signal, the transmission of this packet flow across the network, and then de-packetization at a distant sink. Typically, real-time applications require a minimum of bandwidth to work well. They do not work properly if the minimum of resources is not available. In contrast, elastic applications makes use of the available bandwidth. If the bandwidth is not temporarily available, elastic applications will wait without being severely affected.

Real-time applications that realize a **two-way communication** require a low delay (100s of ms [17, 100]) in order to ensure the interactivity of the application. Real-time applications with **one-way communication** (streaming or stored audio- and/or video) require the limitation of the delay to a certain maximum. These applications use a play-out buffer [33, 133] in order to remove the packet jitter. Therefore, they require an a-priori knowledge about the maximum delay in order to adjust the size of their play-out buffer and are sensitive to a maximum delay. With respect to reliability, real-time applications are loss-tolerant. An interrelation between loss and delay exists: If data are buffered as in streaming audio/video applications with a play-out buffer, then any data arriving before this playback point can be used to reconstruct the original signal, while any data after that point will be useless and the reliability suffers.

Elastic applications are not time sensitive, but require a fully reliable data transfer. The reliability is offered by a reliable transport protocol, such as TCP. Again, there is an interrelation between delay and reliability. When packets are lost, these packets are retransmitted at the expense of an increased delay. However, elastic applications usually tolerate this increased delay up to a certain degree.

Host mobility pertains to all of the three key parameters delay, reliability and packet loss. As it will be described in the coming sections, a mobility scheme can increase the network delay by routing of packets on an indirect path from the application source to the sink. Also, an application experiences a handover by a service interruption and data loss. A service interruption due to handover of 100s of ms impairs the interactivity of two-way real-time applications. One-way real-time applications are pertained if the service interruption exceeds the *play-out time* of packet buffered in the play-out buffer.

Elastic applications tolerate the service interruption caused by handover up to a certain degree. Since transport protocols ensures the reliability of packet loss, elastic applications also tolerate packet loss caused by handover. However, the transport protocols such as TCP are designed and optimized to cope with losses caused by network congestion. Their utilization in mobile networks with handover is an open question.

Tab. 2.1 lists the reliability, bandwidth, and timing requirements of popular and emerging Internet applications. In summary, the following application requirements are identified:

- Provision of low network delay between application sources and sinks for real-time applications,
- Provision of low service interruption and data loss handover for real-time applications,
- Provision of maximum delay for streaming real-time applications,
- Minimal signaling overhead, in particular on the wireless link,
- Support of horizontal as well as vertical handover,
- Simplicity, ease of deployment.

Other functional requirements for mobility support are:

Support of heterogeneous end systems. Future wireless networks will support a variety of mobile hosts with different equipment. This equipment may include screens, video and sound support, input devices (touch screens, pointer, keyboards, voice recognition), data processing capabilities, storage and network devices. In particular, low-end, light-weight end systems will have only limited memory and processing power, ruling out solutions that have substantial memory or CPU requirements. A mobility scheme must support all these end systems. Moreover, mobile hosts will be equipped with more than one network interface; the *best* interface can

Application	Data loss	Bandwidth	Time Sensitive
File Transfer	No loss	Elastic	No
E-mail	No loss	Elastic	No
Web documents	No	Elastic (few kbps)	No
Real-time audio/video	Loss-tolerant	Few Kbps – 1 Mbps	Yes (100s of ms)
Stored audio/video	Loss-tolerant	Same as above	Yes (Few seconds)
Interactive games	Loss tolerant	Few Kbps – 10 Kbps	Yes (100s of ms)
Financial Applications	No loss	Elastic	Yes and No

Table 2.1.: Requirements of selected applications [100]

be chosen based on current environment and application. With the progress of software radio technology wireless interfaces are able to adapt to the current environment and switch between different modes if demanded/beneficial.

Support of heterogeneous access networks. Future wireless networks will be characterized by a variety of wireless access networks coexisting with each other, each offering different compromises between cost, bandwidth, and coverage. No single technology will be able to encompass all usage scenarios. Additionally, nodes will be able to switch between such access networks at arbitrary times (so-called vertical handover). Therefore, a mobility scheme cannot assume that access network parameters or even organization remains constant before and after a handover: handing over from wireless LAN to second generation cellular networks will radically change the communication environment.

Provision of location privacy and anonymity. Ubiquitous network access makes privacy concerns an urgent requirement. Since an IP address represents a host identifier as well as its physical location, the temporary IP address of a user betrays the users current location. Tracking this address and even distributing it to third parties to ensure reachability harms people's privacy. Moreover, the unique identification of a user could be used to compromise the user's privacy.

Small signaling overhead. Signaling for location updates and handover may consume a considerable portion of the wireless bandwidth. This includes the signaling overhead for soft state refreshes of network routing state. A scheme for host mobility support must restrict itself to a small signaling overhead.

2.5. Mobile IP: The Classical Solution for Mobility Support in IP Networks

Mobile IP (MIP) represents the classical solution for mobility support in IP-based networks. It is an accepted standard in the Internet Engineering Task Force (IETF) community. It comes in two different flavors: Mobile IPv4 and Mobile IPv6. The motivation of Mobile IP is to offer a pure network-layer solution for mobility support and to isolate higher layers from mobility. In particular, it aims at preserving continuous TCP connections even though handover causes IP address changes. The IP routing mechanisms remain unchanged.

Mobile IP was first introduced for Internet Protocol Version 4 (IPv4) [129, 131]. The main idea is that a mobile host owns an IP home address and gets assigned in addition a temporary Care of Address (CoA) in a foreign network. A correspondent host addresses the mobile host via its IP home address. Mobile IP adds two new instances to the network infrastructure: A Home Agent (HA) and Foreign Agent (FA) are executed in IP routers. Routing is performed by address translation and tunneling: Suppose a Correspondent Host (CH) wishes to send packets to the mobile host and sends it to its home address. The home agent intercepts and tunnels the packets to the CoA of the mobile host. Tunneling a packet means its encapsulation by the home agent. The foreign agent decapsulates the packets and forwards them via local mechanisms to the mobile host. For the reverse direction from the mobile host to the CH, the mobile host is allowed to send packets directly. This is referred to as *triangular routing.*

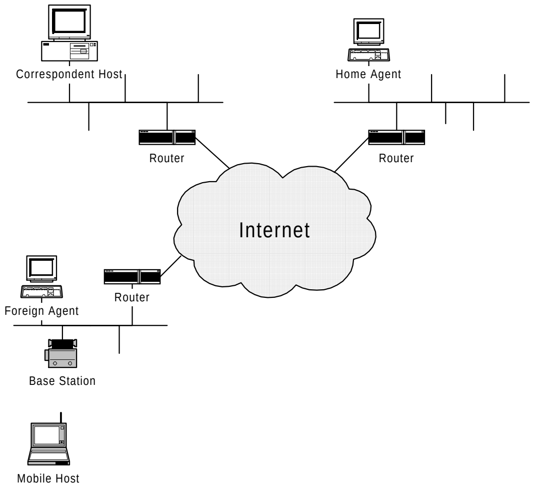


Figure 2.6.: Mobile IP network architecture

The agents periodically send advertisements on the wireless links in order to advertise the offered service and to provide a means for handover detection by the mobile hosts. When the mobile detects that is has moved to a new visited IP subnet (e.g. by Lazy Cell Switching (LCS)[2], Prefix Matching[3], Eager Cell Switching (ECS)[4] [131]) and has obtained a new temporary IP address, it registers its new IP CoA with the new foreign agent. The foreign agent in turn relays the registration to the home agent which binds the new CoA to the mobile host's IP home address. Following packets arriving in the home network will be interpreted by the home agent and tunneled to the mobile host‘s new CoA.

In general, the mobility support in Internet Protocol Version 6 (IPv6) [96] is based on the same main principles as Mobile IP for IP version 4. But in Mobile IPv6 a mobile host is able to create its own CoA using its link-local address and automatic address configuration (combine advertised subnet prefix with own hardware address). Mobile IPv6 introduces two new IPv6 destination options header, namely a *Binding Update* and a *Binding Acknowledgment.* The destination options header is one of the so called *IPv6 extension headers* that is treated only by the final destination. The mobile host can directly send a *Binding Update* in the same packets carrying effective traffic to its correspondent host (see Fig. 2.7). The correspondent host can then learn and cache the new mobile host's CoA. As a result of this mechanism, a host, when sending a packet to any IPv6 destination, must first check if it has a binding for this destination.

[2] The mobile host detects the handover due to expiration of the lifetime of the last received agent advertisement

[3] The mobile host receives a new advertisement with a different network prefix. This can be interpreted as a handover

[4] When the mobile receives multiple advertisements from different foreign agents it may select one of them.

- If a mobile host entry is found, the host sends the packets directly to the CoA indicated in the binding, using an IPv6 routing header. This special extension header forces the datagram to follow a predetermined route which has two hops. The first hop is the CoA and the second hop is the home address of the mobile host. This avoids the routing of packets via the home agent and packets can be sent directly to the mobile host. The mobile host receives the packet and *forwards* it to the next hop specified in the routing header. The next (and final) hop is the home address of the mobile host and the packet is *looped back* inside the mobile host. Now the packet can be processed in the same way as if the mobile host were at home.
- If no binding is found, the packet is sent to the mobile host's home address. The home agent intercepts the packet and tunnels it to the CoA as previously described.

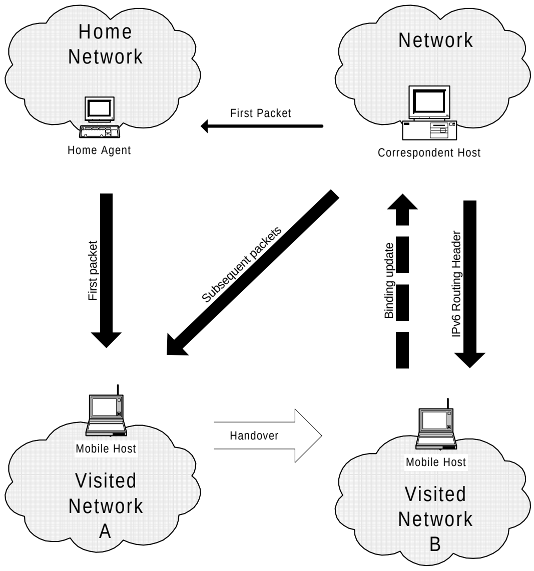


Figure 2.7.: Binding update in Mobile IPv6

2.6. Weaknesses of Mobile IP

Mobile IP suffers from a number of problems. The identification of these problems have resulted in the development of extensions and modifications of the classical Mobile IP as well as in the development of alternative approaches.

The first problem is caused by triangular routing: It adds delay to the traffic towards the mobile host. Measurements have shown that Mobile IP increases the delay by 45 % in a campus network [177]. For two way- real-time communication, this delay is – frequently experienced – not acceptable.

Second, encapsulation adds an overhead of about 20 bytes (IP-in-IP encapsulation [128]) to each packet. In comparison to the packet size of typical real-time applications, such as audio, the overhead is remarkable. For example, the voice codec G.723.1 [80] has a data rate of 5.3 kb/s with a frame size of 20 bytes. With a protocol overhead for IPv4 (20 bytes), UDP (8 bytes), and Real Time

Protocol (RTP) (12 bytes), a packet has a length of 60 bytes. Due to the encapsulation the total packet length increases by 33 %.

Third, triangular routing poses a problem due to ingress filtering. Ingress filtering is a common security mechanism in routers. The mechanism checks for topologically incorrect IP addresses. In Mobile IPv4, the mobile host uses its home address as the source address to send an IP packet directly to the correspondent host. When a router, such as the access router of the current IP subnetwork, examines this packet, then the router detects that the packet seems to originate from outside of the subnetwork. Therefore, these packets will be discarded. A solution is to use reverse tunneling; however, the mobile host does not know a priori that the packets will be discarded by routers due to ingress filtering.

Fourth, Mobile IP may cause a high handover latency. In Mobile IP, a mobile host sends a binding update to the home agent. When the home agent receives the binding update, the home agent tunnels the packet to the new foreign agent. While handover messages are transported to the home agent and back, the mobile host is not connected to the network. When the delay between the mobile host and the home agent is large, then the service interruption is inacceptable. Moreover, during the handover process packets destined for the mobile host will be misdirected to the old foreign agent. These packets get lost. The main reason for this performance problem is that in Mobile IP the point for rerouting is located in the home network that might be very distant from the current location of the mobile host.

Fifth, in Mobile IP the mobile host sends a binding update to the home agent each time the mobile host re-registers for refreshing the binding update in the network. When the current location of the mobile host is distant from the home agent the aggregate signaling traffic traverses many routers in the network and poses a considerable load.

Some of the weaknesses are solved in Mobile IPv6. Nevertheless, in view of the high number of installed systems using IPv4 and the unclear evolution of networks from IPv4 to IPv6, a mobility solution for IPv4 is needed. Moreover, some of the problems – such as the performance problems with handover – still exist in IPv6.

2.7. Review of Existing Alternative Approaches to Unicast-Based Mobility Support in IP Networks

Mobility support in IP networks has been the subject of intensive research efforts beyond Mobile IP for several years. Therefore, it is worth reviewing the following approaches: hierarchical Mobile IP, Mobile IP extensions by MosquitoNet, Reverse Address Translation (RAT), HAWAII, Cellular IP, IAPP, Mobile People Architecture, ICEBERG, and Extended SIP Mobility. These approaches attempt to supplement or to replace the classical solution for mobility support Mobile IP.

In order to work out the basic assumptions behind the schemes, the motivation to develop a new approach, the required mobility infrastructure as well as the addressing and routing concept are emphasized.

Hierarchical Mobile IP. The Mobile IP extension of *hierarchical foreign agents* [62, 63, 70] addresses a drawback of Mobile IP: If the distance between the foreign agent and the home agent is large, the signaling delay for the registration may be long, which then results in long service disruption and packet losses. Therefore, the foreign agent functionality is distributed to several routers. These foreign agents can be configured in a tree-like structure. The *Highest Foreign Agent (HFA)* is the root of the hierarchy, the *Lowest Foreign Agent (LFA)* is close to the mobile host on the path between the mobile host and the home agent. *Intermediate foreign agents* are on the path between the highest and the lowest foreign agent. This foreign agent that belongs to the old and the new path at an handover event is called the *switching foreign agent.* The classification of the foreign agents is conceptual only. The hierarchy may collapse down to a single foreign agent, as in the original Mobile IP approach. The approach works as follows: The LFAs send announcements including their own address and the address of the next higher level. When a mobile host first arrives at a visited domain, it sends a registration request to the LFA which creates an unacknowledged binding update and forwards the registration request upwards to the next higher foreign agent. This initial registration request creates an address binding in every foreign agent on the path, and finally in the home agent.

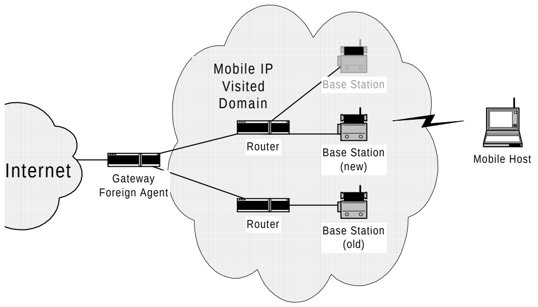


Figure 2.8.: Network architecture for hierarchical Mobile IP

When a handover occurs the mobile host generates a registration request that is forwarded by the LFA. At some point the *switching foreign agent* receives the request and detects that a binding update already exists but is coming from a different LFA. This is interpreted as a local handover. The *switching foreign agent* replies to the mobile host with a *registration reply* message.

MosquitoNet Extensions of Mobile IP. Other extensions have been proposed by the MosquitoNet group in [177]. The goal of these extensions are to use Mobile IP most efficiently and flexibly on mobile hosts. Mobile IP is extended by the following functionalities:

- The regular IP routing table is extended by a Mobile IP specific routing table.
- The Mobile IP home agent can manage multiple CoAs for a single mobile host simultaneously and bind a flow to a certain interface.
- The protocol supporting registration between the mobile hosts and the home agent is extended.

First of all, these extensions allow to decide whether to use transparent mobility support or not. It is argued that Mobile IP implies some remarkable overhead which should be avoided when transparent mobility support by indirect routing is not necessary. Second, the mobile host can decide whether to use triangular routing or bi-directional routing. Mobile IP route optimization (triangular routing) fails when router ingress filtering is used: Packets are dropped when they do not carry a topologically correct IP source address. Therefore, a mobile may use the more robust bi-directional tunneling although it implies an additional overhead. The information whether to use transparent mobility or indirect routing, as well as triangular or bidirectional tunneling, is contained in the Mobile IP specific routing table on a *per socket* basis.

In the context of this approach the support of multiple interfaces in a mobile host is essential. Each interface carries a temporary IP address. A flow can be bound to a specific interface. This is done with the help of a socket option. For transmission, the route lookup has been modified, so that only routes with that specific interface are considered. For reception of data, a flow-to-interface binding (flow is recognized by IP addresses and port number) is sent to the Mobile IP home agent which forwards datagrams to the appropriate CoA. The handover is similar to Mobile IP, but extends the protocol by an update of the flow-to-interface binding in the Mobile IP home agent. The extension is mainly intended for vertical handover of mobile hosts with multiple network interfaces.

Reverse Address Translation (RAT). The RAT approach [147] is motivated by the limited deployment of Mobile IP. It is intended to simplify mobility support in order to break the *chicken and egg-trap* between the lack of applications which require mobility support and the poor deployment of Mobile IP. The RAT approach can be considered as a tradeoff: On the one hand it dispenses with the requirement to maintain TCP connections. On the other hand overhead is decreased and most of the traffic can be routed directly. Moreover, the inventors of RAT argue that implementation of Mobile IP functionality is operating system dependent (e.g. registration, tunneling, etc.), whereas RAT aims at a solution that is independent of the operating system.

In the RAT approach the mobile host owns an IP home address and acquires a temporary IP address in the foreign network. The RAT approach adds new entities to the home network: a registration server and a RAT device. The network infrastructure remains unchanged. In particular, there are no mobility-specific entities required in the foreign network. The RAT approach applies Network Address Translation (NAT) [149]. NAT is an Internet paradigm that has been widely applied recently, for extending the IP address space in IP version 4, but also supports the security when used in firewalls.

The RAT approach works as follows: Suppose a correspondent host wishes to send a packet to the mobile host and directs it to the mobile host's home address. In the home network, the RAT device intercepts the packet and performs a network address translation. Therefore, it replaces the destination address with the mobile host's temporary address and the source address with the address of the RAT device. Then, the packet is sent directly to the mobile host without tunneling. In the reverse direction, the mobile host sends a packet to the RAT device, which in turn performs the address translation and sends it to the correspondent host. This scheme is referred to as *reverse address translation.* One of the main advantages of this approach is that the indirect routing is deployed for correspondent host initiated sessions only. When the mobile host initiates the session, it will use its temporary address (which is topologically correct) and communicate with the correspondent host directly[5], and thus no indirect routing via the home network is required. This results in shorter routes and does not increase the packet length by encapsulation.

Handoff Aware Wireless Access Internet Infrastructure (HAWAII). HAWAII [134, 135] was proposed since Mobile IP results in high control overhead and high latency for local mobility. Also, HAWAII eases the usage of resource reservation protocols (such as RSVP) in a mobile environment, where a mobile host acquiring a new CoA on each handover would trigger the establishment of a new resource reservation. The HAWAII approach extends Mobile IP and addresses its limitations.

[5] The authors argue that most of the sessions are initiated by the mobile host.

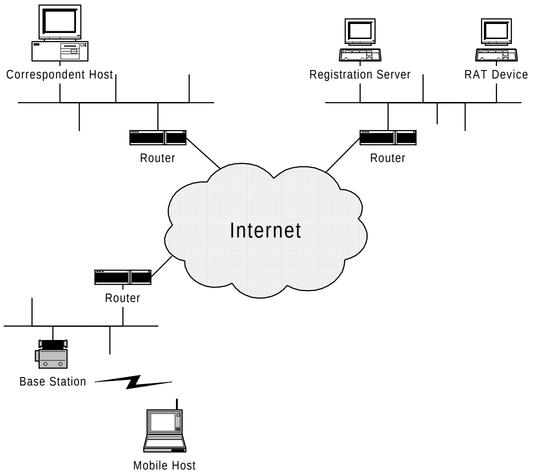


Figure 2.9.: RAT network architecture

HAWAII defines a *domain*. This is a division of the wireless access network under the administrative control of a single authority. The domain consists of routers and access points. All of them are mobility-enabled by supporting HAWAII-specific signaling in order to optimize routing and forwarding. The router interconnecting the HAWAII domain and the Internet core network is called *foreign domain root router*. Each access point has Mobile IP foreign agent functionality.[6]

In the HAWAII approach mobility is separated between *intra-domain* handover and *inter-domain* handover. For both cases different mechanisms are defined. The first case is supported by HAWAII and the second case by Mobile IP. Both cases will be explained below.

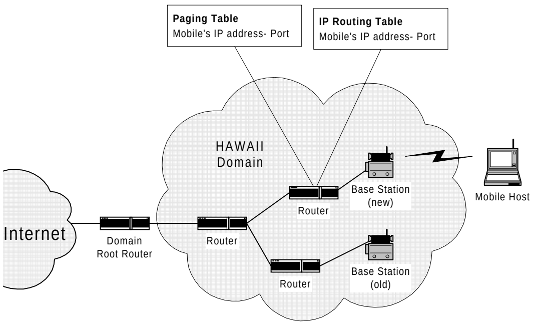


Figure 2.10.: HAWAII network architecture

In the HAWAII approach a mobile host has a home domain (similar as the home network in Mobile IP) and a temporary unicast IP address. The home domain may support the HAWAII protocol. When the mobile host is in a foreign HAWAII domain the temporary IP address is assigned once to the mobile host and does not change as long as the mobile host stays in

[6] Without decapsulation.

the domain. No address translation mechanism is required, and the Mobile IP home agent is not notified of the mobile host's movement. Instead, connectivity is maintained by using dynamically established paths in the foreign HAWAII domain based on host entries in the routing table of selected routers. Thus, a HAWAII enabled access network does not rely on IP routing in the sense of routing based on the network's portion of the IP address. Instead, the IP address is interpreted as a unique identifier and *not* as a location identifier.

As mentioned above, for global mobility support HAWAII reverts to traditional Mobile IP mechanisms. At first, the case is considered where the mobile host is within the HAWAII home domain. In this case the mobile host carries a unicast IP address.[7] When the mobile host powers up, it sends a Mobile IP *registration message* to the present access point. The access point then propagates a HAWAII *path setup message* to the *domain root router* using a configured default route. Each router in the path between the mobile host and the domain root router adds a forwarding entry for the mobile host. Finally, the domain root router acknowledges to the access point. The access point in turn replies the Mobile IP registration to the mobile host. Packets for the mobile host are sent to the domain root router based on the subnet's portion of the mobile host's IP address. The packets are routed within the domain using the host-based forwarding entries. It is important to note that the entries are soft-state being kept alive by periodic hop-by-hop messages.

When the mobile host moves within the HAWAII domain the mobile host registers with the new access point by sending a Mobile IP *registration request.* The new access point then sends a HAWAII *path setup update* message to the old access point. The old access point performs a routing table lookup for the new access point and adds a forwarding entry for the mobile host's IP address. Then the message is sent to the upstream router. This router performs similar operations. If the router receiving this message is the crossover router[8], then this router adds a forwarding entry to the new access point and packets for the mobile host are sent to the new access point. The path via the old access point will time out. This scheme is called *forwarding path setup* scheme since the HAWAII path setup update message is sent from the new to the old access point, and the old access point forwards packets to the new access point only for a limited time. This scheme is optimized for networks where the mobile host listens/transmits to only one access point simultaneously. An alternative scheme is the *Non-Forwarding* scheme, which is optimized for networks where the mobile host is able to listen/transmit to two or more access points simultaneously. In this path setup scheme the *path setup update* message travels from the new access point to the old access point via the crossover router. Thus, packets are not forwarded from the old access point.

In order to interact with Mobile IP the mobile host is assigned a co-located CoA from its HAWAII foreign domain. A correspondent host directs the packets to the mobile host's home address. The Mobile IP home agent intercepts the packets and tunnels them to the HAWAII *foreign domain root router* with the network portion of the outer IP address. This foreign domain root router and the following routers forward the packets according to its host-based routing entries.

The HAWAII approach differentiates between active and idle users as well as appropriate states for the mobile host. For an active user the network knows the mobile host's current access point, and for an idle user the network only knows the access point approximately, such as a set of access points. When packets for an idle mobile host arrive, the network *pages* the mobile to determine the mobile's current access point.

[7] The authors argue that this address might be quasi-permanent.

[8] This router has a route to the old and the new access point via the same interface.

Cellular IP. The Cellular IP approach [157] envisions a networking environment with ubiquitous computers where highly mobile hosts often migrate during active data transfers and the users expect minimal disturbance to ongoing sessions. The authors argue that Mobile IP is not an optimal solution, because it is optimized for macro-level mobility and relatively slowly moving hosts. Moreover, it is stressed that Mobile IP does not scale for a large number of mobile hosts, since every handover between Mobile IP foreign agents generates a binding update irrespective of the fact whether the mobile host is idle or active.

The Cellular IP approach proposes a hierarchical mobility management which separates *global* from *local* mobility. For global mobility, Mobile IP is applied to support handover across the Internet backbone. To support local mobility within the Cellular IP access network, regular IP routing is replaced with routing of packets hop-by-hop via lookup in specific tables. The tables apply soft-state principles which are referred to as caches.

In a Cellular IP network a mobile host is assigned a unique identifier which is used to route packets. It is not required that a mobile host has an IP CoA. For simplicity reasons, the unique identifier is an IP address (e.g. home address) that makes inter-working with Mobile IP more easy. However, this is not really required, since within the Cellular IP access network no IP routing is performed.

For mobility support Cellular IP adds a *gateway router* and *Cellular IP nodes* to the network infrastructure. A gateway router interconnects the Internet backbone and the Cellular IP access network. The Cellular IP nodes are located in the Cellular IP access network and can be considered as access points working at network level. They execute the Cellular IP protocol. It is not required that they are equipped with a wireless interface (if not, they act as a regular network node).

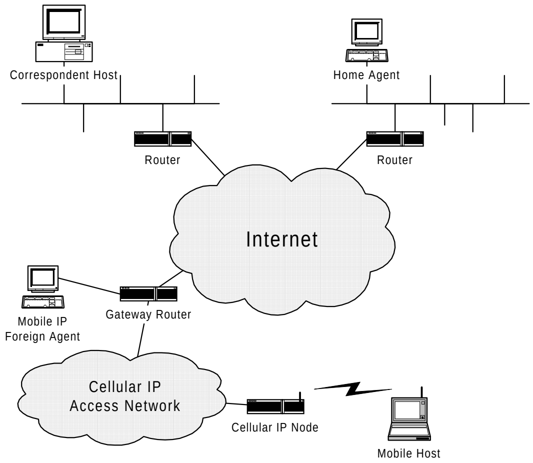


Figure 2.11.: Cellular IP network architecture

The global mobility support in Cellular IP is provided straightforward by Mobile IP. The Gateway router is co-located with a Mobile IP foreign agent. The mobile host registers the gateway's IP address with its Mobile IP home agent. Packets from a correspondent host are first routed to the Mobile IP home agent and then tunneled to the gateway. The gateway de-tunnels packets and forwards them towards the access points. As long as the host is interconnected to the same access network, local mobility is hidden from the agent in the gateway router.

The local mobility support works as follows: Inside the Cellular IP access network, nodes are provided with a *Paging Cache (PC)* and a *Routing Cache (RC)*. Both contain mappings between mobile host IDs and node ports (Output port similar to a router port) on a soft-state basis. Paging caches are available in a few nodes. A paging cache is updated by data originating from the mobile host (data packets or specific signaling packets). The paging cache is used to locate a mobile host when there is no routing cache entry. In that case, the Gateway Router caches the IP data packets in order to send a paging packet to the mobile host across the Cellular IP nodes. The mobile host replies to that paging packet and creates routing cache entries in every node along the route. Now, the cached IP packets can be sent along this route without address translation and tunneling. paging cache and routing cache entries are cleared by timers, with different timeout values: The routing cache timeout is on the order of several IP packets, whereas the paging cache timeout is set according to the handover frequency. Thus, an idle and active mobile host can be managed separately with different data bases.

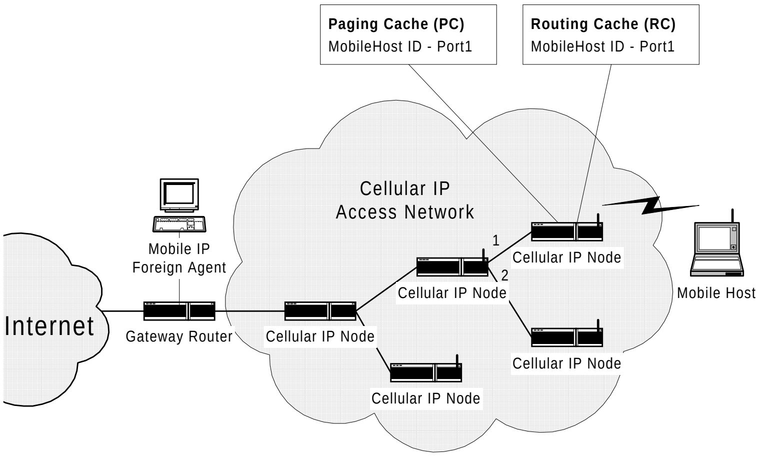


Figure 2.12.: Cellular IP access network architecture

When a handover occurs two cases have to be considered. In the first case the mobile host generates a *route update* packet when it enters the new cell in order to update the route caches in those nodes where the old and new route diverge. After the route caches are updated, data packets are sent to the new location of the mobile host via the new route. For a limited time the old and the new routing cache entry can exist in the routing cache and data packets are sent via the old and the new route. This is used for *semi-soft* handover. In the second case, the routing cache entry in the Gateway was cleared, triggered by a timer. Then a new paging packet is generated to locate the mobile host. This explicit search causes a small delay in sending packets, but it allows longer timeouts decreasing the amount of signaling packets.

Inter Access Point Protocol (IAPP). The IAPP [110] defines, how access points of an IEEE 802.11 network communicate with each other to support handover of mobile hosts. The protocol facilitates the support of handover within the boundaries of an IEEE 802.11 network which can be regarded as local handover working below the network layer. For global handover an other mobility solution is required (e.g. Mobile IP).

An IEEE 802.11 system achieves a spatial coverage common to local area networks by connecting wireless cells by a wired backbone, termed *distribution system*. The internals of the distribution system are not defined in the IEEE 802.11 standard. The IAPP provides a mechanism by which access points can exchange information, even for access points from different vendors.

The IAPP consists of two modules – the announce protocol and the handover protocol. The announce protocol is for informing other access points that a new access point has become active and other management tasks. The handover protocol is used to inform the old access point that a mobile host is taken over by another access point, update the old access point's registration table to forward frames destined for the mobile host appropriately. The handover procedure is directly tied into the IEEE 802.11 re-association procedure at link layer.

The IAPP protocol is mainly developed to provide inter-operable interaction between access points from different vendors for mobility support within a IP network/subnetwork.

Mobile People Architecture (MPA). The main goal of the Mobile People Architecture [7, 105, 140] is to maintain a person-to-person reachability while preserving the mobile user's person privacy.

In the Mobile People Architecture a user is identified by a *Personal Online ID*. Additionally, a user is addressed by *Application Specific Addresses*. Mobility is supported by mapping the Personal Online ID to Application Specific Addresses (ASAs).

In the Mobile People Architecture a new entity is added to the network. This entity is called a *personal proxy* and acts as a *person level router* (The person level is added to the communication layer model on top of the application level.) The personal proxy tracks the user's current reachability, converts media, and forwards data to a specific end system. It is located in the mobile host's home network (if any), or is offered by a trusted third party server.

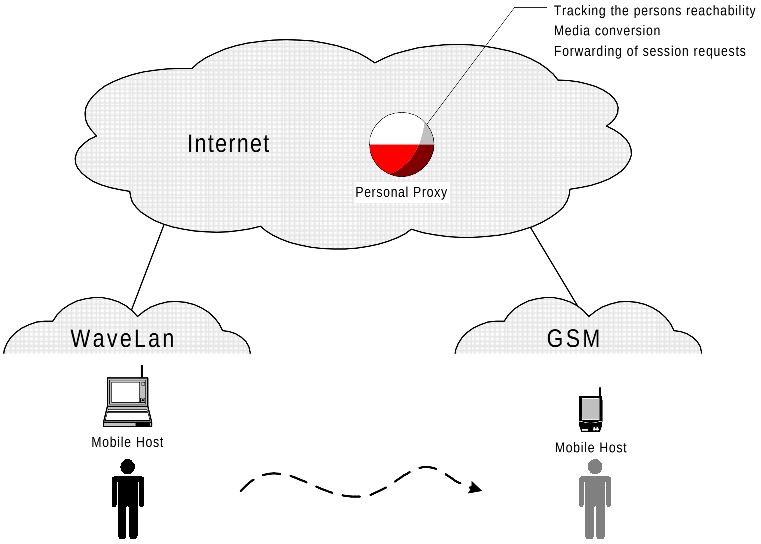


Figure 2.13.: The Mobile People network architecture

When a user wishes to communicate with the mobile *person* a call (call is regarded as a kind of session) is directed to the Personal Proxy, and then to the mobile person's preferred end system. When the reachability of the mobile person changes, the proxy state is updated by the tracking agent. The update can be done in a scheduled manner, manually or automatically.

It is assumed that local mobility is handled within the access network and hidden from the Personal Proxy. The case that a user changes the end system can be regarded as vertical handover. Then the user updates the Personal Proxy (manually or automatically) and new calls will be directed to the user's new ASA. The case that a user changes the ASA while receiving service is not being considered.

Internet Core Beyond the Third Generation (ICEBERG). The motivation of the ICEBERG project [161] is the current diversity of access networks, end systems, and services; in particular, traditional telephony services and data services. Therefore, the ICEBERG project aims at supporting personal mobility in the sense of seamless access to services independent of the access network and end system. It is intended to give the control of the communication to the callee, and not to the caller.

In ICEBERG, a user can be uniquely identified (by means of a *unique-id*). Additionally, the user is associated with one or several *service-ids* (e.g. phone number, email address, IP address). To achieve mobility the *unique-id* is mapped to the *service-id*.

In general, the ICEBERG network architecture consists of the Internet Core and several different access networks (e.g. GSM, PSTN, WLAN). At the interface between the core network and an access network an Iceberg Access Point (IAP) transforms services (media converter). Additionally, ICEBERG adds service agents to the core network: preference registries, Personal Activity Tracker (PAT), and extended naming services. The preference registry stores user preference profiles that can be modified by user interaction or by the PAT which gives inputs about location information.

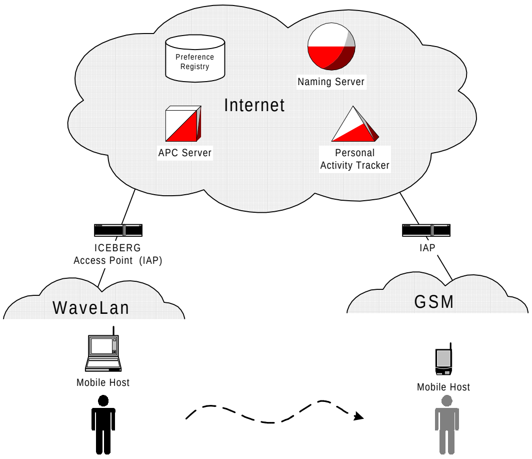


Figure 2.14.: ICEBERG network architecture

Suppose a correspondent user wishes to call the mobile user. The call is routed to the IAP. In the access point a name service lookup is performed, the preference registry of the called user is located and the preferred end system is determined. After that the call is established via the correspondent interface. A service conversion (e.g. fax to jpeg) is executed in the IAP.

The ICEBERG approach focuses on user mobility between several access networks. It is implicitly assumed that host mobility is transparently supported in the access networks by technology specific handover schemes (e.g. for GSM, IEEE 802.11, etc.).

Extended SIP Mobility. Extended SIP Mobility [162] is an mobility approach that utilizes the application level signaling capabilities of the Session Invitation Protocol (SIP) protocol [74]. The motivation of the extended SIP mobility can be found in drawbacks of the Mobile IPv4 approach. The authors argue that for real-time traffic over IP, which is mostly RTP [144] over UDP traffic, there is a need for fast handover, low latency, and high bandwidth utilization. Mobile IPv4 suffers from indirect communication which increases the delay and causes an overhead due to tunneling, which on its part decreases bandwidth utilization.

The extended SIP mobility approach introduces mobility awareness at a higher layer than the network layer. SIP already supports user mobility, and the approach is meant to extend SIP as an application-layer signaling protocol in order to support end system mobility.

The main assumption behind the extended SIP mobility approach is that a mobile user is identified by a unique address (e.g. user@realm). This unique address is mapped to the current IP address of the mobile user's end system. No explicit home IP address is required. SIP introduces a SIP agent on the user's side and a SIP server (SIP redirect server or SIP proxy server) and location server to the network infrastructure.

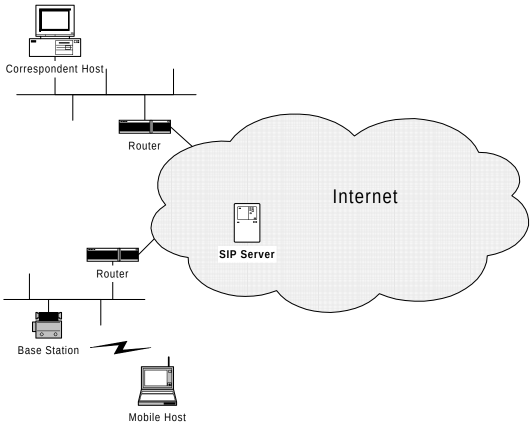


Figure 2.15.: Network architecture for extended SIP mobility

User mobility is supported by means of the original SIP protocol: When a user wishes to initiate a session, an invitation is directed to the SIP server which in turn queries the location server for the current IP address of the mobile user's end system. The SIP server sends the invitation to the called user. The invitation contains the IP address of the callee. If the mobile user moves, the location server is updated, and new sessions will be set up to that new IP address.

End system mobility with this scheme is mainly understood as an increased roaming frequency and as a change of an IP address during an ongoing session. Assuming that a session is already established, then the mobile registers the new temporary address with the location server and the mobile re-invites the correspondent host with the same session identifier and the new temporary address (in the contact field of the SIP message). The session can be continued, although the IP address has changed.

It is important to note that SIP does not support TCP. Therefore, extended SIP mobility supports UDP traffic only. For TCP traffic it is proposed to use Mobile IP. It is argued that both approaches can coexist: For TCP traffic Mobile IP is applied and for UDP traffic the extended SIP mobility approach. For the simultaneous usage of network interfaces the MosquitoNet approach of a *mobile routing table* [177] is adopted.

2.8. Summary

In summary, the approaches to mobility support in IP networks based on IP unicast can be divided into three main categories as shown in the diagram in Fig. 2.16.

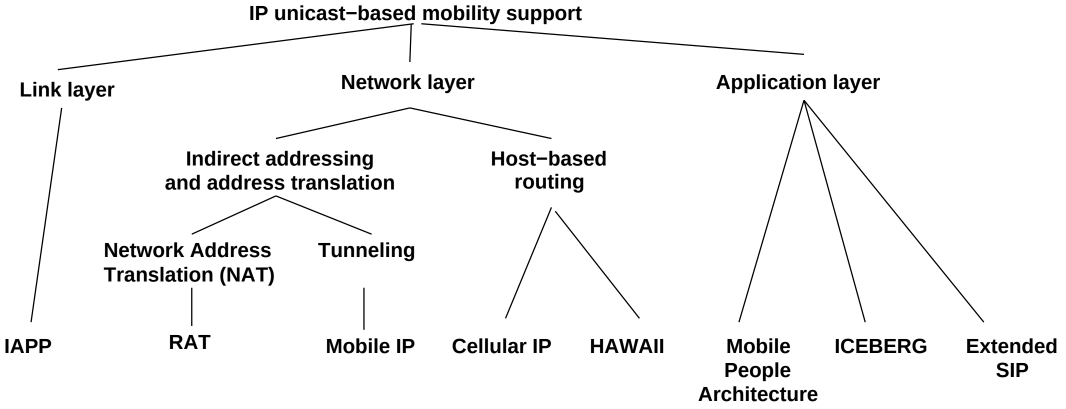
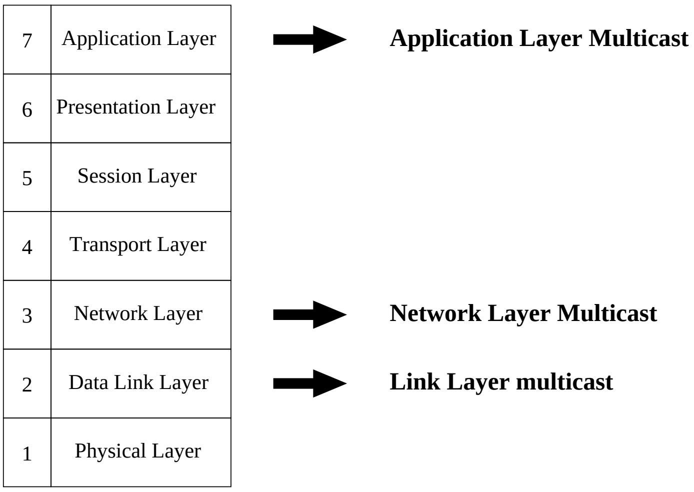

IP unicast−based mobility support
Link layer
Network layer
Application layer
Indirect addressing and address translation
Host−based routing
Network Address Translation (NAT)
Tunneling
IAPP
RAT
Mobile IP
Cellular IP
HAWAII
Mobile People Architecture
ICEBERG
Extended SIP

Figure 2.16.: Classification of IP unicast-based mobility approaches

The classical solution for mobility support is Mobile IP. Mobile IP overcomes the general mobility problem by using additional agents in the network to map the mobile host's identity to its current location ensuring that arbitrary hosts can communicate with a mobile host in an uninterrupted way even while the host moves around. Despite this achievement, Mobile IP has been widely criticized for its performance problems and for not matching all possible requirements for a mobility concept. Some of these requirements are technology-driven: The need for higher bandwidths results in the use of ever higher frequency bands with high attenuation and low wall penetration making very small cells a necessity. In highly mobile environments very frequent handovers occur resulting in performance degradation and frequent disturbances of communication. Using different types of cells with different technologies and communication radii, organized into a hierarchical system, could overcome some of these problems but would also result in new problems. Other requirements are user-driven: Examples include different types of access needs (e.g. WB-CDMA offering soft handover capability) or service requirements (low loss versus low jitter). As Mobile IP has been criticized on the grounds of such diverse requirements, other concepts have been proposed that also solve the fundamental mobility problem in a different manner. Approaches applying host-based routing (such as Cellular IP and HAWAII) aim at micro-mobility support and require a complementing solution for macro-mobility. Application-layer mobility approaches provide a scalable solution in combination with network-layer micro-mobility approaches. But they do not provide a general solution for all applications, instead they are specific to particular applications. However, they offer a short-term solution for network-layer micro-mobility approaches. Hence, multicasting-based mobility – being the focus of this thesis – can be regarded as an alternative to these unicast-based approaches.

3. Multicast Fundamentals

In this chapter the fundamentals of multicast-based mobility support are introduced. First, the basic concepts of multicast are explained. Then, three basic approaches to support multicast at different layers of the protocol stack are described: *link-layer multicast*, *network-layer multicast*, and *application-layer multicast* (see Fig. 3.1 and 3.2). Among the approaches, the network-layer multicast is the most important one. Therefore, in the following section the multicast approaches in connection-less networks and in connection-oriented networks are detailed. It is worth noting that the considerations are not restricted to the standardized multicast service models, such as the IP any-source multicast (ASM) or the ATM multicast service models, respectively.



7	Application Layer	Application Layer Multicast
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	
3	Network Layer	Network Layer Multicast
2	Data Link Layer	Link Layer multicast
1	Physical Layer	

Figure 3.1.: Multicast approaches with respect to the ISO OSI reference model

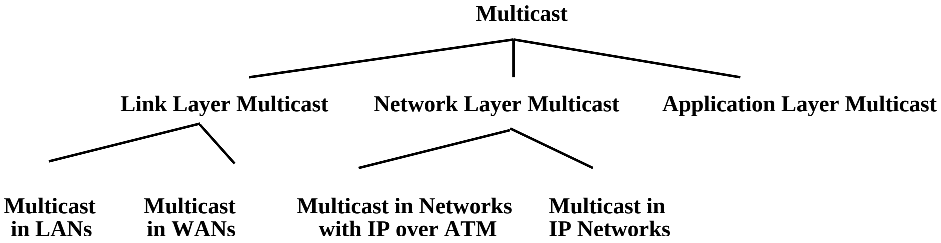


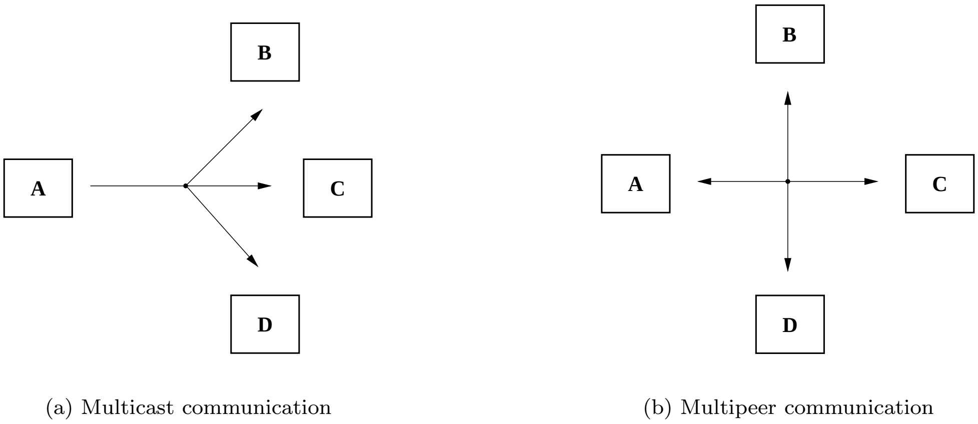
Figure 3.2.: Classification of multicast approaches

3.1. Basic Concepts of Multicast

Formally, multicast is defined as a specific approach of group communication among multiple participants. Group communication can be categorized with respect to the number of senders and recipients [169], where a point-to-point communication is understood as a special case of group communication. Four cases can be distinguished, with the first term in brackets representing the number of senders, the second term the number of recipients:

- Unicast $(1 : 1)$
- Multicast $(1 : n)$
- Concast $(m : 1)$
- Multi-peer $(m : n)$

Multicast is defined as group communication where a single sender sends messages to several (more than one) recipients as shown in Fig. 3.3(a). The network accepts a single message from a sender and delivers copies of the message to multiple recipients at different locations. In the formal definition a communication with several senders and several recipients is referred to as multi-peer communication (Fig. 3.3(b)).



(a) Multicast communication

(b) Multipeer communication

Figure 3.3.: Formal definition of two selected cases for group communication

A communication group can also be characterized by the following features [169]:

Openness. In an open group data can be sent from any sender to the group, whereas it is not necessary that the sender is a group member. In closed groups data can be exchanged between group members only.

Dynamic. A static group does not change its compound during its lifetime, whereas in a dynamic group members can join or leave the group even when communication within the group is ongoing.

Lifetime. Transient groups exist as long as at least a single communication participant belong to the group. A permanent group also exists when the group has no participants at all.

Anonymity. In an anonymous group the identity of the group members is unknown to the other members of the group. In a known group, the members know each other. Either the sender knows the recipients and/or vice versa or all participants know each other at all (including the recipients among each other).

In practice it is convenient to use the term *multicast* also for scenarios with more than one sender (e.g. link-layer multicast, IP multicast). Although this description does not match the formal definition and is less precise, the term *multicast* will be used for $(1 : n)$ and $(m : n)$ communication throughout the thesis. If it is necessary to distinguish both cases, $(1 : n)$ communication will be referred to as *multicast in the narrow sense.*

A specific method to realize group communication is the emulation of multicast by means of *replicated unicast*: Assuming n recipients, a sender sends a single message to each recipient and a total of n messages.

In comparison with unicast communication, multicast has a number of benefits:

First, multicast reduces the amount of bandwidth in the network required to transport data to multiple recipients. On each part of the path from the sender to the recipients a multicast message is transported only once. Only that network node where the paths to different recipients diverge duplicates the message. Particularly, for highly utilized networks (low bandwidth / high data rates) multicast is required since an *emulated* multicast with replicated unicast might even exceed the available bandwidth.

Second, multicast saves processing power in the source and facilitates the fact that a service may scale to extremely large audiences. With multicast an application generates a message only once, and this message is also sent on a link only once. The delivery of data to multiple recipients can be realized with *replicated* unicast as well: The source generates messages according to the number of recipients. But, the usage of multicast reduces the processing power in the source in comparison with replicated unicast. For extremely large audiences, the usage of multicast becomes a requirement since the processing power of the source exceeds its processing capabilities.

Third, the usage of multicast minimizes the delay in sessions with distributed interactive applications, for example network games. In such applications, the network delay caused by replicated unicast to all session participants imposes an application impairment. Multicast minimizes this network delay [46].

Fourth, a multicast source does not have to know the population of the receivers. The sender does neither know the number of subscribed receivers nor their identity. Hence, in the multicast source node the amount of state is small in comparison to replicated unicast.

There exist a number of applications that make use of or can seriously benefit from multicast. They can be categorized into four types [47], typically working on the basis of *one–to–many* or *few–to–few*:

- *Multicast file transfer*: Transmission of data (typically a large amount of data) from one location to multiple locations. With a growing amount of data and number of receivers the requirements on bandwidth and duration of the file transfer are not manageable and require multicast. Multicast file transfer supports web–caching, distributed databases and remote logging.

- *Audio/video distribution* (Web–casting): A source transmits real–time audio and/or video over the Internet to a single or to several destinations simultaneously.

- *Push applications* (Information delivery): Allows individual users to select channels. Information is pushed to the users on these channels upon appearance of proper events.

- *Audio– and video–conferencing and group collaboration applications*: These applications are based on mechanisms that are also used for Web–casting. Additionally, they allow an interaction between various users. The applications are usually *few–to–few*.

The utilization of multicast for host mobility in IP-based networks creates a new category of multicast application. Its basic idea will be explained in Chapt. 4.

Multicast can be provided at different protocol layers with respect to the OSI reference model.[1] Link-layer multicast, network-layer multicast and application-layer multicast are detailed in the next section.

3.1.1. Link-Layer Multicast

The link-layer, layer 2 of the seven layer OSI model (Fig. 3.1), is responsible for the transport of data over a particular link. In local area networks (LANs), links interconnect hosts, in wide-area networks (WANs), links are defined from one location to another.

Link-layer Multicast in Local Area Networks (LANs)

LANs are typically characterized by shared media with a connection-less service where all hosts are attached to the same physical medium. Each host carries a unique Medium Access Control (MAC) address, sometimes called a *physical* address. There are different types of MAC addresses: *unicast*, *multicast*, and *broadcast* MAC addresses. A frame sent on the network carries a MAC address. The hosts are able to listen to each frame sent in the LAN. Examples of such networks are IEEE 802.3 (Carrier Sense Multiple Access/Collsion Detection (CSMA/CD)) [90], 802.4 (token bus) [91] and 802.5 (token ring) networks [92].

With link-layer multicast the broadcast capability of a physical medium is exploited. A host which is member of a certain multicast group accepts frames for a proper associated MAC multicast address. For IEEE 802.3 networks today's network interface cards are able to accept frames on a per address basis. These network interface cards store MAC addresses and accept frames for each of these addresses.

Fig. 3.4 illustrates the link-layer multicast in a Local Area Network (LAN): Hosts A–E are interconnected by a broadcast-capable medium. Host A sends a frame on the medium using a multicast MAC address. Host B and E have stored this address and choose to receive the frame.

Using multicast on a physical network with non-broadcast medium is both more complex and less efficient. It often requires a central network node that performs distribution to each receiver either in a one-to-one or one-to-many connection.

Multicast in LANs with MAC bridges and switches is coordinated by registration and forwarding functionalities which are defined in the Generic Attribute Registration Protocol (GARP) and the GARP Multicast Registration Protocol (GMRP) [89].

Link-Layer Multicast in Wide Area Networks

In comparison to link-layer multicast in LANs, wide area networks (WANs) are not based on shared media. Therefovere, these approaches emulate the behavior of shared media. Examples for link-layer multicast in a WANs are multicast in *Frame Relay*, *Switched Multi-Megabit Data Service (SMDS)*, and *Asynchronous Transfer Mode (ATM)*. Since multicast neither in Frame Relay nor in SMDS have ever been deployed remarkably, those are not detailed here. The main constraint of link-layer

[1] Open System Interconnection, reference model for internetworking.

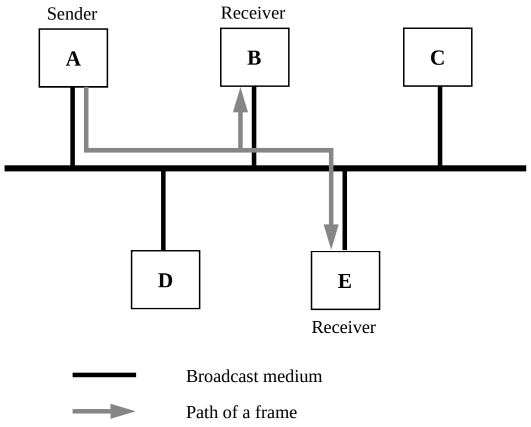


Figure 3.4.: Link-layer multicast in local area networks

multicast in Frame Relay and SMDS is the fact that the multicast group is statically set up by the network and can only be changed by a reconfiguration of the network [67].

ATM is a connection-oriented cell-switching technology. In ATM, a Virtual Circuit (VC) – Permanent Virtual Circuit (PVC) or Switched Virtual Circuit (SVC) – are established among nodes that emulate actual physical links. Multicast in ATM networks is based on a sender-oriented model where the sender establishes a multicast connection to all receivers. Therefore, a tree is generated with the sender as a root and receivers as leaves. Data are sent from the root node along the tree. The tree is set up by establishing a connection between the sender and a single receiver. Then further receivers are added step by step. All modifications of the group membership have to be notified to the sender that adds/drops receivers from the tree. This sender-oriented model requires the sender to know all receivers explicitly since in ATM no notion of an ATM multicast address exists to address a multicast group indirectly.

Today, there exist relatively few native ATM applications making use of ATM services. Nevertheless, ATM is prevalent in today's WANs and Internet backbones where the high bandwidth of the ATM's underlying cell switching technology is utilized to carry IP traffic. Therefore, the mapping of IP traffic to the multicast of a connection-oriented technology, such as ATM (layer 2), is an important issue. Several approaches to multicast with IP over ATM will be briefly described in section 3.2.2.

3.1.2. Network-Layer Multicast

The network layer, layer 3 in the ISO OSI reference model, figures out the optimal path to route packets through various links to the end points. Network-layer functionality is usually performed by routers using routing algorithms to determine optimal routes to the destination. For multicast at the network layer IP multicast is the most important approach. Although other protocol stacks besides TCP/IP support network-layer multicast, such as Appletalk and DECNet, the deployment of these protocols is decreasing rapidly. Hence, these approaches will not be introduced in the thesis, and for the discussion of network layer the terminology of TCP/IP protocols will be used exclusively.

In general, the use of one of the two strategies can provide multicast at the network layer: Based on host addresses and based on specific group addresses (see Fig. 3.6).

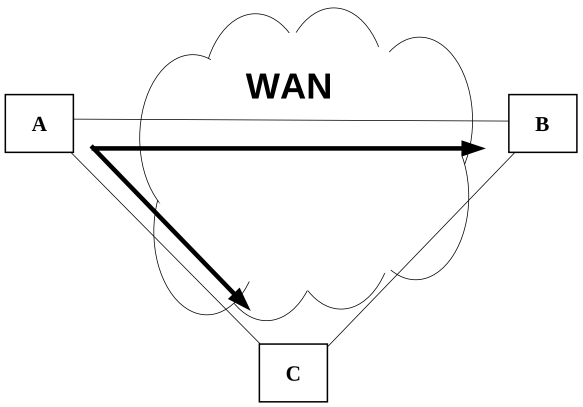


Figure 3.5.: Link-layer multicast in wide area networks

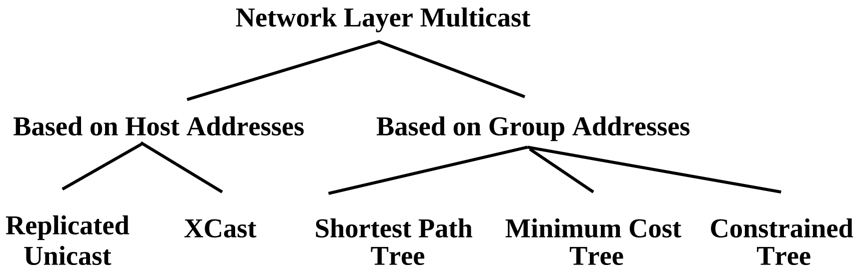


Figure 3.6.: Strategies for Network-Layer Multicast

Network-Layer Multicast Based on Host Addressing

In the first strategy the sender needs to be aware of the receiver addresses belonging to a particular multicast group and uses the receivers' unicast IP addresses. The sender generates either multiple messages each carrying the unicast IP address of a certain receiver (replicated unicast), or a single message carrying the unicast addresses of all receivers. In the second case, each router on the path examines the destination addresses of the message and performs routing functions similar to unicast routing, except that they duplicate the message if the route to the receivers diverges in that router.

Network-Layer Multicast Based on Group Addressing

The second strategy is based on specific group addresses, e.g. addresses that have been reserved from the IP address pool as described in Sect. 2.2. Unicast IP addresses (class A, B and C addresses) are applied for point-to-point communication and have a host and network component. In contrast, a class D IP address for multicast has one (not subdivided address space indicating the multicast group. In IPv4 the multicast address space range from 224.0.0.0 to 239.255.255.255.

For network-layer multicast a host needs to inform the nearest router supporting IP multicast (e.g. the designated multicast router in the host‘s network) of its membership in particular multicast groups. Messages will be forwarded by routers on multicast distribution trees up to the receivers as the leaves. For establishment of multicast distribution trees the multicast routers cooperate and use certain algorithms to create multicast distribution trees [126]:

Shortest Path Tree algorithm. With a *Shortest Path Tree (SPT)* algorithm, a tree is rooted at the sender and spans all receivers so that the distance between the sender and each receiver along the tree is a minimum. For dynamic trees either the *Distance Vector* algorithm or the *Link State* algorithm is used [85].

In the *Distance Vector* algorithm, the router attached to the sender broadcasts to its neighboring routers the fact that it is directly attached (distance 1). The neighboring routers, in turn, compute the distance to the sender and select the minimum distance among possibly multiple alternatives. Each of these routers again broadcast its distance to its neighboring routers. Then this process is repeated.

The *Link State* algorithm is based on *Dijkstra's shortest path* algorithm for routing of unicast packets. Each router in the network has a complete view of the topology. In this algorithm the routers flood a change in the state of a directly connected link as soon as such a change occurs. For example, if a directly connected link becomes inactive, a router immediately broadcasts this information to all neighboring routers and so forth. Once a router has a complete view of the topology, it applies *Dijkstra's shortest path* algorithm to compute the shortest path from the sender to each receiver.

Minimum Cost Tree algorithm. The intention of the *Minimum Cost Tree* algorithm is to minimize the overall costs of a tree. There are two types of algorithms: *Minimum Spanning Tree* algorithm and *Minimum Steiner Tree* algorithm.

In the *Minimum Spanning Tree* algorithm a tree spanning the sender and the receivers is computed in which the overall costs of the tree are minimal. In addition, this tree should *not* include any node which is not a member of the group.

In the *Minimum Steiner Tree* problem the tree is *not* restricted to group members only – instead it is allowed that a tree includes the group members and, additionally, non-group members so that the overall costs of the tree are minimal. The *Minimum Steiner Tree* is NP-complete and some heuristics have been proposed.

Constrained Tree algorithm. The *Constrained Tree* algorithm is based on the idea to minimize not only the overall costs of a tree, but the end-to-end-delay as well. Therefore, each link is assigned two distinct metrics: cost and delay. The *Constrained Tree* algorithm aims at computing the minimum cost tree which does not have any path that exceeds a certain delay bound.

The basic algorithms are used (or proposed to be used) by multicast routing protocols in the Internet. They will be discussed in section 3.2.1.

3.1.3. Application-Layer Multicast

In principle, application-layer multicast is based on an application's capability to self-organize into a logical overlay network and transfer messages along the edges of the overlay network using unicast transport services. Each application communicates only with its neighbors in the overlay network. By forwarding packets from neighbor to neighbor multicast forwarding is performed at application layer.

As an example, suppose a network with hosts A–E interconnected by a mesh of links in which all hosts are members of a single multicast group as shown in Fig. 3.7. The applications in the hosts create an overlay network which is marked by the thick lines. When host A sends a message to the multicast group, this message is forwarded via the overlay multicast tree directly to host A–D. For host C the message is forwarded by host D[2].

The membership of multicast groups is managed at the application layer as well: Applications interested in joining a multicast group send the IP address of their hosts to a *multicast master*, an application executed in a dedicated host or router of the overlay network. The master determines the appropriate router for forwarding to the host of the particular application, and informs and configures routers. The forwarding of data is based on the IP unicast routes of the routers. The duplication of data (in order to forward the data on different path of the overlay network to the multicast receivers) is executed at the application layer.

Typical examples for application-layer multicast are *NARADA* [31, 32], *OverCast* [94], *ScatterCast* [29], and *JungleMonkey* [76].

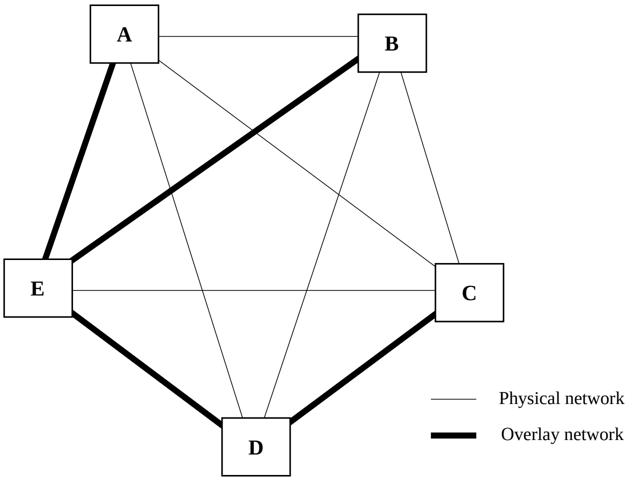


Figure 3.7.: Overlay network on top of a physical network for application layer multicast

Application-layer multicast has a number of attractive features:

- Application-layer multicast requires no changes of the existing Internet infrastructure, only additional servers to create the overlay network. There is no need of network-layer multicast support. This reduces the complexity of router configuration and management by setting up forwarding trees at the application layer. Moreover, this offers an accelerated deployment of a multicast service.

- Application-layer multicast does not rely on unique group identifiers and therefore there is no need for a global address allocation as for IP multicast. Many of the application-layer multicasts use a URL-like group identifier.

- Traffic control mechanisms (flow control, congestion control) for unicast traffic can be exploited. There is no need for specific multicast transport protocols as for IP-layer multicast. Most of the application-layer multicast approaches uses standard TCP as a transport protocol between the hosts of the overlay tree.

[2] More precisely, the nodes in Fig. 3.7 are routers.

- The edges in the overlay network can be assigned link costs of an application-specific metric. This enables to set up application-specific multicast trees. For example, many applications may find the latency as the most appropriate metric. Other applications may prefer a high bandwidth, high delay path to a low bandwidth, low delay path.
- Application-layer multicast allows more flexibility in customizing some aspects, e.g. error recovery, flow control and security (e.g. access control) on an application-specific basis. For example, *ScatterCast* uses delay as the routing cost and builds shortest path trees from data sources. *OverCast* explicitly measures available bandwidth on an end-to-end-path and builds a multicast tree by maximizing the available bandwidth from the source to the receivers. *NARADA* uses a combination of delay and available bandwidth and prioritizes available bandwidth over delay when selecting a routing path.

In summary, application-layer multicast is regarded as an alternative architecture to deploy multicast in the current Internet. It has a number of benefits over IP-layer multicast. Most of them arises from the challenges of the IP multicast for which no clear solution has emerged so far. However, since the support of this multicast is implemented at user space, this is less efficient than implementation at kernel level. Application-layer multicast can be regarded as a short-term solution of network-layer multicast as long as network-layer multicast has not found wide deployment.

3.1.4. Summary

In the latter sections, it was pointed out that multicast can be provided at the link layer, network layer, and application layer. It can be summarized that two approaches provide mechanisms to solve the fundamental mobility problem in IP networks, i.e. *link-layer multicast (in WANs)* and *network-layer multicast based on group addresses*. In principle, both approaches offer location-independent addressing and routing. In *network-layer multicast based on group addresses*, the IP address is used as a host identifier only and does not identify the location, whereas packets are routed by means of a multicast distribution tree established by multicast routers. In IP networks with *link-layer multicast*, the unicast IP address is mapped to a link-layer address and IP packets are transparently transported to the network layer by means of the link-layer. Hence, the IP address reflects only the host identifier and not the location of the host.

The two remaining approaches – *application-layer multicast* and *network-layer multicast based on unicast* provide location-dependent addressing and routing and hence, they do not solve the fundamental mobility problem. Nevertheless, they can be utilized to improve mobility support. It will, however, be shown in the next chapters that these approaches can be utilized for mobility support. It should also be noted that *link-layer multicast in LANs* is naturally limited by LAN boundaries and therefore cannot be used for mobility support among LANs.

Since *network-layer multicast based on group addressing* and *link-layer multicast in WANs* and could be identified as basic classes for multicast-based mobility support, existing service models and protocols for both approaches will be detailed in the next section. In the following, more general terms are used. The former approach is referred to as *multicast in connection-less networks*, the latter approach *multicast in connection-oriented networks.*

3.2. Multicast Services and Protocols

3.2.1. Multicast in Connectionless Networks

In general, multicast in connection-less networks is based on the principles explained in Sect. 3.1.2. In this section, the service model of the classical IP multicast is described and its problems are identified. Approaches for a future IP multicast are derived, which have been recently proposed and can, potentially, help to overcome the problems.

Service Model of the Classical IP Multicast (Any-Source Multicast, ASM)

The classical IP multicast is based on a *Any Source Multicast (ASM)* service model. Basically, it consists of four features: I) A multicast group is a set of receivers identified by an IP class D address. II) A group is dynamic, a host can dynamically join or leave an IP multicast group. Join and leave operations are principally receiver-driven. III) A group is open, a sender does not need to be a member of a multicast group, each host is allowed to send to a multicast group. IV) The group is anonymous, neither receivers nor senders do know the members of the group (number and identity).

In order to join or leave a multicast group the Internet Group Management Protocol (IGMP) [55] is used.[3] Multicast routers periodically transmit *Host Membership Query* messages to determine which multicast groups have members on their directly attached network. When a host receives an IGMP *Host Membership Query* message, it responds with a *Host Membership Report* message for each group to which it belongs. If multiple hosts in a subnet belong to the same multicast group, redundant reports are suppressed by means of a random back-off timer mechanism: A multicast router does not need to know the exact number of hosts in the group in that subnetwork; it needs to know only that at least one host belongs to that multicast group. This feature reduces the multicast signaling load. When a host joins a multicast group for the first time, it may send an unsolicited *Host Membership Report* without waiting for an IGMP Membership Query message.

Multicast Routing Protocols for the ASM Service Model

The multicast routing protocols for the ASM service model are Distance Vector Multicast Routing Protocol (DVPRP), Protocol Independent Multicast – Dense Mode (PIM-DM), Multicast Extensions to Open Shortest Path First (MOSPF), Protocol Independent Multicast – Sparse Mode (PIM-SM) and Core–Based Tree (CBT). Multicast routing protocols use either a *broadcast and prune* or an *explicit join/leave* mechanism. *Broadcast–and–prune* protocols are commonly called *dense-mode protocols* and always use a reverse shortest path rooted at the source. Explicit-join/leave protocols, commonly called *sparse mode protocols*, can use either a reverse shortest path or a *shared tree.* The shared tree uses a *core* or a *rendezvous point* to bring sources and receivers together.

In the following the multicast routing protocols for the ASM service model are briefly described.

Distance Vector Multicast Routing Protocol (DVMRP). DVMRP [159] is based on the principles of the RIP distance-vector unicast routing protocol [104] and extends the mechanisms to multicast. In principle, DVMRP is based on a *broadcast–and–prune* algorithm. It uses *Reverse Path Forwarding* (RPF) to establish an IP multicast distribution tree. When a router receives a packet on an interface, the reverse path to the source is checked to determine whether it is the shortest path to the source. If the packet has been delivered on the the shortest path

[3] IGMPv1 is specified in RFC 1112 and defines a protocol between multicast routers and hosts on a subnet attached to that router. IGMP has been extended twice but neither of these extensions have achieved official standard status yet.

from the source, the router copies the packet to all interfaces except one – the interface back to the source of the packet. Otherwise, the packet is discarded. The RPM mechanism uses a unicast routing protocol, that is part of DVMRP. A multicast router that has no members for a particular multicast group, sends a *prune* message back up the distribution tree. When the upstream router receives a *prune* message, it stops forwarding of multicast packets on the corresponding interface. Similarly, a *graft* message grafts a new branch to the distribution tree. Prunes and grafts have a limited lifetime. When the lifetime expires, the *broadcast–and–prune* algorithm is repeated and the distribution tree re-established.

Multicast Extensions to Open Shortest Path First (MOSPF). MOSPF [112] provides multicast extensions to the OSPF unicast routing protocol [113]. OSPF is based on link-state principles. Each OSPF router has a complete view of all links in the network and calculates the routes from itself to all other destinations. For multicasting, the OSPF *Link State Announcements* (LSAs) are augmented by group membership information and the router maintains a link state database with additional group membership information. When an initial multicast datagram arrives in a router, the router determines the source subnetwork in the MOSPF link-state database and calculates a source-based, shortest path distribution tree by using Dikstra's algorithm. Because the location of the group members within the topology is known, the distribution tree is established through that router so that branches lead only to subnetworks containing members of this group.

Protocol Independent Multicast – Dense Mode (PIM-DM). PIM comes in two flavors: Protocol Independent Multicast - Dense Mode (PIM-DM) and Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-DM [3] was developed as a companion protocol to PIM-SM as a set of routing protocols with the same message types that work efficiently in both sparse and dense mode environments. PIM-DM is based on a *broadcast–and–prune* algorithm similar to DVMRP. It initially broadcasts data packets and then prunes the branches where no members of the group exist. Unlike DVMRP with its own included unicast routing protocol, PIM-DM relies on an existing unicast routing protocol to perform RPF checks. Therefore, is is not dependent on any particular unicast routing protocol. There exist some other minor differences between PIM-DM and DVMRP which result in a simpler design of PIM-DM at the expense of duplicated initial data packets.

Protocol Independent Multicast – Sparse Mode (PIM-SM). PIM-SM [43, 51, 54] was designed in combination with PIM-DM to provide a routing protocol set with common packet formats and to operate efficiently in sparse and dense mode environments.[4] PIM-SM is a *shared tree* protocol, the multicast distribution tree is the same for all members of a group, regardless of the source. In contrast, a dense mode protocol creates a new distribution tree for each source. In PIM-SM members of a group join a *Rendezvous Point (RP)* where receivers *meet* sources. When a host joins a group using IGMP to notify its directly attached router, the router joins the multicast delivery tree by sending an explicit *PIM Join* message hop-by-hop toward the RP. The designated router of the source knows how to reach the RP and forwards packets to the RP by encapsulating the multicast packet into a *PIM-Join* unicast message. The RP decapsulates the unicast packet and forwards the multicast packet towards the multicast delivery tree to the group members. Moreover, the RP returns a *PIM-Join* message to the source's designated router and allows future forwarding from the source to the RP without encapsulation.[5] When a group member leaves a group, the designated router sends a *PIM*

[4] Nevertheless, PIM-DM and PIM-SM are separate protocols and run in separate regions, which must not overlap.

[5] In fact, the RP joins the shortest path tree of source.

Prune message to the RP and the branches are pruned back. PIM-SM also offers the optional switching to a shortest path tree once it begins receiving packets from the source. This switch can be triggered, for example, if the data rate of the source exceeds a predefined threshold of data rate. However, the routers can be configured to never switch to the source-based tree.

Core Based Tree (CBT). CBT [10, 11] uses a single bi-directional shared tree for a multicast group. Similar to PIM-SM, the CBT protocol employs the information contained in the unicast routing table without requiring the presence of any specific unicast routing protocol. Since PIM-SM has evolved from CBT, there exist many similarities between both protocols: Both rely on a shared tree with a root node, which is called *Core* in CBT. Also, the bootstrap mechanism to elect a core among the multicast routers is very similar to PIM-SM. In CBT a host joins a multicast group by IGMP. The designated, CBT-aware router issues a *Join Request*. If the *Join Request* encounters a router that is already on the group's shared tree before it reaches the core router, that router sends a *Join Ack* back to the source. Once a new branch is established, each child router monitors the status of its parent router with a keep-alive mechanism, the CBT *Echo* protocol. If the link to the upstream router fails for any reason, the downstream branches are torn down by sending a *Flush Tree* message. The multicast routing entries in the routers maintain hard state. Therefore, a multicast tree must be explicitly torn down.

Category	DVMRP	PIM-DM	MOSPF	PIM-SM	CBT
Tree type	SPT	SPT	SPT	Shared/SPT	Shared
Directivity of trees	Uni	Uni	Uni	Uni	Bi
Multiple sources	No	Yes	No	Yes/No	Yes
Number of trees in multiple sources	S	1	S	S	1
Router state	O(SxR)	O(SxR)	O(SxR)	O(R)/O(SxR)	O(R)
Use of core	No	No	No	Yes	Yes
Join mechanism	B&P	B&P	B&P	EJ	EJ

Table 3.1.: Brief comparison of the routing protocols for the ASM service model

A brief comparison of the routing protocols for the ASM service model is shown in Tab. 3.1. The following abbreviations are used: SPT stands for shortest path tree rooted at the source, whereas the shared tree refers to a single tree per multicast group shared by the sources. With respect to directivity, a tree can be *uni-directional (uni)* or *bi-directional (bi)*. *S* and *R* refer to the number of sources and receivers, respectively, and are used to express the expense of router states. The join mechanism can either be based on *broadcast and prune (B&P)* or *explicit-join (EJ)*.

Availability and Deployment of the Classical IP Multicast

In principle, multicast in IP networks is available and could be deployed in today's networks. A number of applications exist, such as the session directory tool *sdr* for announcement and joining a multicast session, video and audio conferencing tools, e.g. *vic*, *NetMeeting*, *vat*, tools to record and play audio- and videos, e.g. *vcr*, shared text editors, e.g. *nt*, shared white-boards, e.g. *wb*, tools for polling and rating, e.g. *MPoll*, and many others. Most of them are open software. Protocols for multicast management (e.g. IGMPv2 [55]) belong to the protocol stack of standard operating systems, like Microsoft (MS) Windows, Linux, Solaris etc. Multicast routing protocols are part of the standard configuration of commercial routers, whereas router manufacturers prefer different types of multicast routing protocols, such as PIM (CISCO), DVMRP (Bay Networks), MOSPF (Proteon). Also, the Multicast Backbone (MBone) [5] represents a long-term, large-scale experiment operating since 1992 based on IGMP and DVMRP. In this context a great number of experiences in successful deployment of multicast services could be gained and problems identified. These experiments are continued in the *Internet 2* employing PIM-SM, MBGP and MSDP as multicast routing protocols (see below).

In spite of this, the classical IP multicast with the ASM service model has seen slow deployment. There are some technical reasons for this:

Multicast address allocation. In the current IP multicast service model, senders cannot reserve addresses or prevent another sender from choosing the same address. Hosts of different multicast sessions using the same multicast address receive unwanted traffic. This results in inefficiency and can create application inconsistencies since packets from other sessions have to be processed and dropped. If multicast were to become more popular, address collisions would become a serious problem and a global address allocation mechanism would be needed. Currently, there exist four alternatives for such a mechanism: the Multicast Address Allocation Architecture (MAAA) [154], static allocation and assignment (GLOP) [107], per-source allocation as proposed by EXPRESS [82] and IP version 6 multicast addressing [72]. The MAAA architecture is a complex protocol suite for dynamic address allocation interconnecting hosts, routing domains and multicast address allocation servers. GLOP uses identifiers of Autonomous Systems as the basis for restricting multicast addresses available to domains. IP Version 6 introduces a drastically increased address space and makes sufficient unique multicast addresses available, which reduces the risk of address collision.

Scalability. Unlike unicast addresses, multicast addresses are not structured and allow no aggregation of routes. This results in a higher number of routing entries with mostly long network prefixes allowing fewer host addresses. Similar problems have been solved in unicast networks by route aggregation and hierarchical routing [99].

Multicast security. Security can be regarded as consisting of four components: authentication, authorization, encryption and data integrity.[6] The ASM service model does not mandate any authentication and authorization. In particular, any host is able to create a multicast group and to force an address collision. Furthermore, any host is able to join a multicast group and receive data not destined to that eavesdropper. Finally, any host is able to send unwanted traffic to a certain multicast group potentially wasting resources in the network and receivers. Source authentication and data integrity is possible through services provided by *IPsec* [98], but not receiver authorization. Moreover, IPsec does not prevent sources from sending, it just allows receivers to drop unauthenticated packets after they have been received. For encryption, application-level key management is regarded as a potential solution. However, most of these problems are still the subject of research.

Charging. It is not possible to charge for multicast traffic by means of the usual model for unicast traffic. For unicast traffic the *Input data rate* R is the basis for charging, and it is assumed that a user with an *Input date rate* R generates a traffic of data rate R . For multicast it is not possible to use this *Input date rate* R as the basis for charging since multicast packets are replicated in the network and a higher data traffic is generated depending on the size of

[6] For authentication hosts are forced to prove their identity. Authorization is the process of allowing authenticated hosts to perform specific operations. Encryption ensures that eavesdroppers cannot read data on the network. Data integrity ensures that data have not been altered in transit.

the multicast group and their distribution over the network topology. Additionally, today's IP multicast does not offer a measure for the multicast group size. This might prevent an Internet service provider from offering a multicast service. Without a multicast service offered by a service provider, a source would have to use replicated unicast and would be charged according to the usual unicast charging model for a bandwidth of $k * R$ where k represents the number of receivers.

Multicast Inter-domain Routing. Multicast routing protocols are typically provided in routing domains, as with unicast routing. Different domains are connected by inter-domain protocols. Multiprotocol extensions of to Border Gateway Protocol (BGP) [139] (namely the Multicast Border Gateway Protocol (MBGP) [13]) can be used to distribute information about routes to multicast sources between domains. However, MBGP does not provide mechanisms to interconnect trees of different domains when group members are spread over multiple domains. In this context, a near-term solution has been proposed, the Multicast Source Discovery Protocol (MSDP) [106]. Given that PIM-SM is the only sparse-mode protocol with significant deployment, the design of MSDP is strongly influenced by PIM-SM. MSDP interconnects the PIM-SM RPs in different domains; and if a source in a particular domain becomes active, the RP in this domain sends a message to the RPs in other domains. This solution does not scale with the number of senders since every RP in every domain must be informed about every source.

Reliable transport and congestion control. Originally IP multicast was designed to support unreliable transport of IP packets. This might lead to two main problems: First, some of the sent packets do not reach all of the receivers. Second, multicast applications sending with uncontrolled data rate can overwhelm the network resources, cause congestion in the network and starve unicast applications. To solve this problem, multicast transport protocols must support reliable packet transport and congestion control. For unicast communication these demands are met by TCP. For multicast transport protocols a number of approaches already exist, e.g. Reliable Multicast Transport Protocol (RMTP) [127] and others, which mainly avoid *feedback implosion*[7] and (unwanted) retransmissions. Although multicast transport protocols have already been the subject of research for several years, non of the resulting approaches has been widely deployed.

Alternative Approaches for Multicast in IP Networks

As has been shown before, the classical ASM service model of IP has some limitations, though it is of great flexibility. Recently, several new proposals have appeared that question the classical multicast approach. The development of alternative IP multicast approaches was particularly driven by the *EXPRESS* proposal, which has gained considerable attention in the research community and has motivated new research efforts.

EXPRESS (EXPRESS) proposed in [82] uses a per-source, *channel-based* mode. A channel is a datagram delivery service identified by a tuple (S, E), where (S) is the sender's IP source address and E is the channel destination address (i.e., a class-D address). Only (S) may send to (S, E). Receivers subscribed to (S, E) are not subscribed to (S', E) for some other host (S'). Thus, packets transmitted from two sources to the same address (E) are only sent to receivers subscribed to both channels. EXPRESS uses Express Count Management Protocol (ECMP), a management protocol that maintains the distribution tree and provides mechanisms to efficiently collect information about subscribers, such as source-directed voting and counting. The single source restriction of the

[7] Arrival of acknowledgments from many TCP receivers.

multicast service model simplifies protocol design and implementation while it facilitates additional capabilities including access control, charging and address allocation.

Simple Multicast [12] is a similar proposal. Again, a multicast group is identified by a tuple (C, M), where C is the core router and M the IP multicast address. Unlike EXPRESS, Simple Multicast allows for multiple sources per group. A particular source is chosen as the primary, and the multicast distribution tree is rooted at the host's designated multicast router. Receivers send *join* messages to the source and a bi-directional tree is set up. Additional sources send packets to the primary source.

In fact, it is the definite trend in multicast research to use a simplified multicast service. The EXPRESS approach described above has largely motivated this trend. A future multicast service that realizes a Single Source Multicast (SSM) service model is expected to have the following benefits in comparison to the classical ASM multicast service model [16, 81]:

- The cross-delivery of traffic is eliminated when two sources simultaneously use the same source-specific destination address.
- There is no need for a global IP multicast address allocation, and therefore no inter-host coordination is required.
- A set of protocol mechanisms that are needed for supporting the SSM service model is a subset of what has been needed for the ASM service model. For example, there is no need for Rendezvous Points in the PIM-SM routing protocol. Moreover, the implementation of single source multicast is considered to be easy, since a number of algorithms are already included in protocols of the ASM service model. For example, the shortest-path tree mechanism of the PIM-SM protocol can be easily adapted to realize the SSM service model.
- Due to the restriction of the number of sources, authorization and authentication is simplified. Moreover, unwanted traffic to a multicast group is avoided in the SSM service model.

Explicit Multicast (XCast) [4, 172] is another approach to a multicast service model in IP. The basic idea of *XCast* is to use an explicit list of destinations instead of a single multicast address that identifies the multicast group. The source encodes the list of destinations in the header of the IP packet and sends the packet to a router. Each router along the way parses the header, partitions the destinations based on each destination's next hop, and forwards a packet with an re-created packet header to each of the next hops. If only a single destination is listed in the packet header, the packet is converted into a normal unicast packet. While the routing protocols of the ASM service model are scalable with the members of a multicast group, i.e. support very large multicast groups, these protocols cause high costs in terms of multicast states in routers and signaling between routers. XCast attempts to efficiently support very large numbers of distinct (small) multicast groups. The main benefits of XCast in comparison to the ASM service model are [21]:

- Routers do not have to maintain state per multicast group (or per source and group). This makes XCast scalable in terms of the number of multicast groups since the routers do not need to disseminate or store any multicast routing information for these multicast groups.
- Multicast address allocation is not required.
- No need for multicast routing protocols (neither intra- nor inter-domain).
- No dedicated root nodes of multicast trees (core, Rendezvous Point), and therefore no single point of failure exists. In contrast to shared trees, XCast packets are routed directly (and not via root nodes of shared trees) which increases the efficiency.

- Easy security and accounting. In contrast to the ASM service model, in XCast a source knows the members of the multicast group, which gives the sources the means to e.g. reject certain members or count the traffic going to certain members quite easily. Not only a source, but also a border router is able to determine how many times a packet will be duplicated in its domain. It also becomes easier to restrict the number of senders or the bandwidth per sender.

- Simpler implementation of reliable protocols on top of XCast, because XCast can easily address a subset of the original list of destinations to do a retransmission.

Several proposals of protocols supporting the XCast service model have been made, e.g. [20, 21, 123]

IP Multicast in Networks with Mobile Hosts

For the design of IP multicast protocols, it has been assumed that the hosts are static. The mobility of hosts – either mobile sources or mobile receivers – causes certain problems:[8]

- When a mobile host moves, the visited network may not support multicast. Therefore, the mobile host is unable to re-join the multicast session until it moves to a new subnetwork providing multicast service.

- After moving into a new subnetwork, a mobile receiver experiences a long handover latency if no other receiver is subscribed to that particular multicast group in this subnetwork. In order to re-join the multicast group, the mobile receiver must wait for the next IGMP membership query. The frequency of these queries is typically in the order of a minute causing the mobile host to endure a long delay in re-joining the multicast group.

- Handover of mobile receivers causes an incorrect routing or dropping of packets with multicast routing protocols based on shortest path trees. The reason for this is the Reverse Path Forwarding (RPF) algorithm used to construct the multicast distribution tree in those routers. The multicast router expects packets to arrive from an upstream interface. When a mobile sends packets while away from its home network, the packets will arrive at the router at an unexpected interface. DVMRP drops such packets, while MOSPF forwards them on a wrong multicast distribution tree.

- The Time To Live (TTL) value of multicast IP packets might be set inappropriately while a mobile host is roaming. Usually, the TTL value is set to the intended scope of multicast packets. When a mobile host moves, the actual TTL value might be too small to reach the receivers of the multicast group. If the TTL value is too high, it may cause an address collision with another multicast group so that unwanted traffic will be received.

3.2.2. Multicast in Connection-Oriented Networks

This section describes the service models and protocols for multicast in connection-oriented environments. Two approaches have been standardized: *IP Multicasting over ATM* and *LAN Emulation (LANE)*. An alternative approach is the *MCall* service realized by the CMAP/CMNP protocol suite.

From the description of the ATM multicast in Sect. 3.1.1 could be seen that the multicast service model of ATM is different from the classical ASM service model of IP. The ATM multicast service model does not use group addresses. The service model implies that the sender is aware of the

[8] The provision of a multicast service to mobile hosts is not the focus of this thesis. Therefore, these issues are for information only.

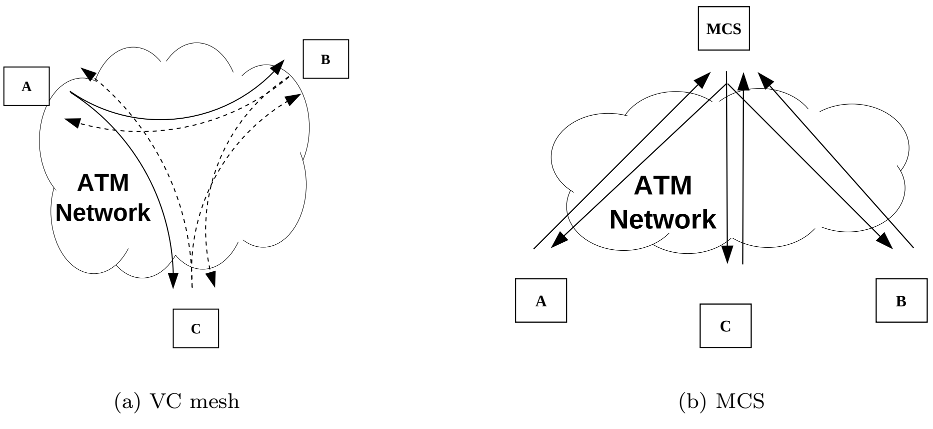
number and identity of the group members. ATM multicast is based on unidirectional point-to-multipoint connections from a sender as the root to the receivers as the leaf nodes. Therefore, multiple senders per multicast group cannot be directly realized. A common feature of the IP ASM and the ATM service model is the fact that ATM end systems can dynamically join and leave the multicast group, whereas a sender is not required to be a member of the multicast group.

IP Multicasting Over ATM

This approach [8] attempts to realize the ASM service model of IP by means of the ATM multicast capabilities. In principle, it maps IP multicast groups on ATM point-to-multipoint connections. It is based on *Classical IP over ATM (CLIP)* [101] and extends the approach by multicast functionality. Consequently, the service provided by *IP Multicasting over ATM* is limited to a *Logical IP Subnetwork (LIS)* representing an IP network/subnetwork as defined by *CLIP*. For assigning an IP multicast address to a list of ATM addresses, a new component is introduced into the network: the Multicast Address Resolution Server (MARS). For forwarding of data two strategies exist: the *VC mesh* strategy and the *Multicast Server (MCS)* strategy.

In the *VC mesh* strategy a point-to-multipoint tree from each sender to the receivers of a multicast group is established (Fig. 3.8(a)). In order to notify membership changes to the senders, a point-to-multipoint control virtual circuit is set up. For example, when a host leaves an IP multicast group, each point-to-multipoint connection needs to be modified to remove the particular ATM end system.

In the *MCS* strategy, multicast data distribution is centralized in a server (Fig. 3.8(b)). A sender generating a packet to an IP multicast group directs the packet to this server. The packet is transported to the multicast server by means of an ATM point-to-point connection. The multicast server re-assembles the cells and forwards the packet on the particular point-to-multipoint connection.



(a) VC mesh

(b) MCS

Figure 3.8.: IP Multicast over ATM

The MARS concept is limited to network boundaries termed LIS, where the virtual circuits between nodes in a LIS can be established directly. *VENUS* and *EARTH* are proposals to supplement the MARS approach. Very Extensive Non-Unicast Service (VENUS) [9] proposes to use MARS for inter-cluster multicast spanning several LIS. Easy IP Multicast Routing Through ATM Clouds (EARTH) [148] extends MARS with QoS and multicast shortcuts.

LAN Emulation (LANE)

This approach attempts to emulate a multicast service as provided in local area networks by link layer multicast (Sect. 3.1.1). In LANE [34, 35, 36, 37, 38], the ATM network is divided into subnets called *Emulated LAN (ELAN)s.* Intra-ELAN unicast traffic is transported by an ATM point-to-point connection and broadcast traffic is served by means of a *Broadcast and Unknown Server (BUS)*, which forwards multicast traffic to all the members belonging to the same ELAN as the sender. Inter-ELAN traffic is forwarded through a router. A multicast packet is either sent by the BUS reaching all ATM end systems in the ELAN or by a dedicated *Selective Multicast Server (SMS)* which allows to selectively choose a list of receivers in an ELAN. In both cases a point-to-multipoint connection is established with the server as the root and the receivers as leaves. A multicast sender directs a packet to the server through a point-to-point connection. The server reassembles the cells and forwards the packet on the point-to-multipoint connection. It is worth noting that the main idea of LANE is the same as in MCS (Fig. 3.8(b)).

Comparison Between IP Multicasting Over ATM and LANE

IP multicast over ATM and *LANE* emulate multicast by means of unidirectional point-to-multipoint connections. Since in standard ATM no multicast group identifier is provided, the multicast sender needs to be notified of membership changes. Particularly, in the *VC mesh* strategy as described above, the point-to-multipoint tree from each sender to the receivers must be modified and causes a considerable signaling overhead and signaling delay with a high group stability latency. In the *MCS* strategy the signaling load and group stability latency is smaller. However, there is a single entity that manages the multicast groups. In networks with a high number of groups and frequent membership changes this entity becomes the bottleneck for resources and processing of signaling operation and limits its scalability. As will be shown later, the utilization of multicast for mobility requires a multicast solution that is scalable in terms of multicast groups and frequent membership changes. The scalability argument pertains to the LANE strategy as well. Therefore, it can be concluded that the multicast solutions of standard ATM – *VC mesh*, *MCS* and *LANE* – are no appropriate candidate solutions for multicast-based mobility support.

Multi-Point Multi-Connection Call (MCall)

Multi-Point Multi-Connection Call (MCall) represents a completely different multicast service model than that of standard ATM. The features of the service model are: I) A multicast group is represented by a *call.* Basically, a call is a multi-connection communication channel. II) Any host that is member of the call is allowed to send and receive to/from the call (closed call). Irrespective of the open group model, a member can be prevented from sending due to other reasons. III) The membership of the call is dynamic, a host can be dynamically added and dropped. The operations can be executed by the host itself or by a surrogate host. V) Multiple senders in the call are allowed. IV) A call is non-anonymous. The sender knows the members of the call and the members know the other members of the call (at least can acquire information about the members).

The *MCall* service model is realized by the CMAP/CMNP protocol suite [65]. The abbreviations stand for Connection Management Access Protocol (CMAP) and Connection Management Network Protocol (CMNP), respectively. In the CMAP/CMNP protocols a *call* represents a multi-point multi-connection communication channel. As the description implies, a call consists of multiple end points and multiple connections (Fig. 3.9), for example a multi-media communication between multiple participants including video and voice communication. A call can be dynamically changed during its lifetime: The number of participants, the number of connections as well as its bandwidth can be modified. Unlike the ATM multicast model based on unidirectional point-to-multipoint connections (*concast*, or multicast in the narrow sense as defined in Sect. 3.1), a *call* provides multi-peer communication (Sect. 3.1). Hence, the approach is considered in the context of *IP-style* multicast.

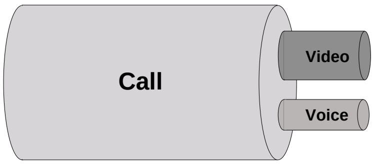


Figure 3.9.: A call composed of two connections (video and voice)

In general, in CMAP/CMNP a network consists of clients and network nodes containing cell switches (Fig. 3.10). A client signals the network to establish a call with other clients by sending control messages. A network node may signal also with other network nodes. CMAP defines the signaling operations between clients and network nodes, whereas CMNP (and its auxiliary protocols) defines the signaling operations among network nodes. Fig. 3.10 illustrates an example network with five clients and four network nodes. The call exists between client 1, 2, 4, and 5. The call is represented by a connection group between the network nodes A, C, and D, whereas the call is routed from A to C via D.

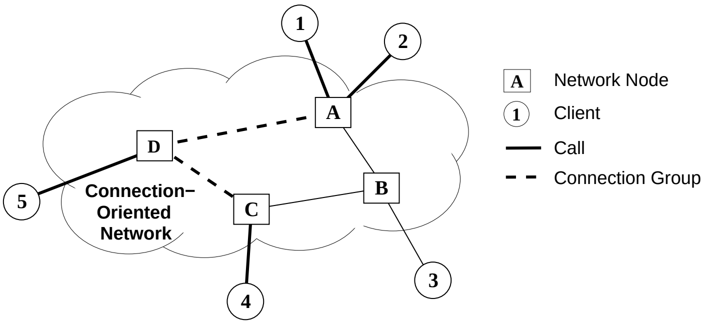


Figure 3.10.: Connection-oriented network with clients and network nodes

Initially, when a call is created, a call has one or more than one connections. The network node that creates the call is designated as the call *owner*. The owner may add connections to or remove connections from the call. When the call is created, it has at least the owner as one of the endpoints of the call. Additionally, endpoints may be added by invitation from the owner, by request from a client not being currently in the call or by request from a third party. Fig. 3.11 illustrates an *Open_Call* operation as an example: End point 1 sends an *Open_Call Request* to the network and specifies a call that includes itself as the owner and the endpoints 3 and 4 as members of the multicast group. The other endpoints are invited by means of an *Invite_Add_Ep Request* and *Invite_Add_Ep Ack* message. Finally, an *Open_Call Ack* message is sent back to end point 1.

While CMAP is the protocol that handles the call operations between clients and the network, CMNP provides functionalities for creation, modification and release of calls within the network. In CMNP, the abstraction of a *connection group* represents the *call* abstraction in CMAP. A main task of CMNP (and its complementing protocols) is the construction of a bi-directional tree of connections through a network with multiple network nodes and links. In CMAP/CMNP, each client has a designated network node. The network node of the owner is used as a core for the

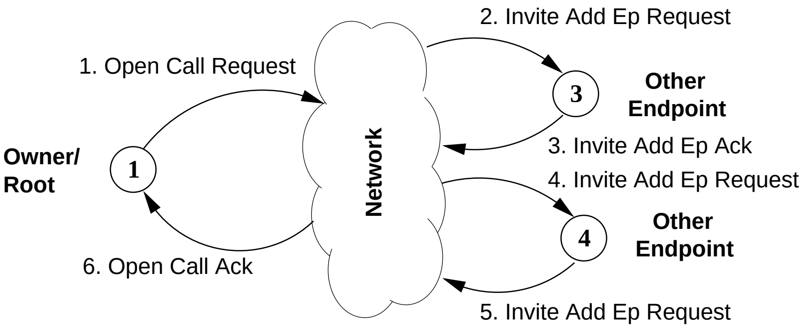


Figure 3.11.: Example CMAP *Open_Call* operation (Simplified example from [40])

multicast tree and can be identified by means of the call identifier. When a new end point is added to the call, the request is forwarded towards the route of the core. If a request encounters a network node already being in the connection group of the particular call, a new branch is added.

Although the CMAP/CMNP approach has been proposed in the context of ATM networks[9], the approach can principally be applied in connection-oriented networks. While the actual implementation of the CMAP/CMNP protocol suite runs on top of a cell-switching technology in the network nodes, the concept and protocol design of the CMAP/CMNP approach can be used for other technologies. In particular, the CMAP/CMNP may be employed on top of connection-oriented optical technologies, such as Wavelength Division Multiplexing (WDM) networks.

3.3. Summary

In this chapter general approaches to multicast services, mechanisms, and protocols have been described. Considering the multicast approaches with respect to the protocol layer – link-layer multicast, network-layer multicast, and application-layer multicast – in detail, it has been concluded that network-layer multicast and link-layer multicast in WANs are principally qualified to provide multicast-based mobility support.

More specifically network-layer multicast can be distinguished into network-layer multicast based on group addresses and based on unicast addresses. Only approaches of the former class provide location-independent addressing and routing. The latter class does not have this feature. Multicast of this class can still be utilized to improve mobility support, but is bound to other basic mobility schemes (such as Mobile IP).

Then, existing multicast protocols in connection-less and connection-oriented network have been considered. A number of protocols can be distinguished: IP multicast routing protocols supporting the any-source multicast (ASM) service model of IP (DVMRP, PIM-DM, MOSPF, PIM-SM, CBT) in connection-less networks, as well as IP multicast over ATM and LANE in connection-oriented networks. Analyzing the drawbacks of the classical ASM service model provided by the existing IP routing protocols and the IP multicast over ATM protocols it has been shown that is it worth investigating alternative multicast services and protocols, such as the SSM service model provided by e.g. PIM-SSM in connection-less networks or the MCall service model supplied by the CMAP/CMNP protocols. These service models alleviate some of the drawbacks of the classical ASM service model

[9] CMAP/CMNP makes use of the virtual circuit concept of ATM, but neither is it based on ATM signaling (User Network Interface (UNI)/Private Network Network Interface (PNNI)) nor does it provide standard ATM services.

and support interesting features that might be useful for multicast-based mobility support, respectively. Tab. 3.2 briefly compares the service models of the main multicast approaches.[10]

Category	ASM	SSM	XCast	ATM	MCall
Group identifier	Multicast group (RG)	Multicast channel (RG,S)	NA (Individual end systems)	NA (Individual end systems)	Call Id (Root node, local id)
Multicast type	Multi-peer (m:n)	Multicast (1:n)	Multi-peer (m:n)	Multicast (1:n)	Multi-peer (m:n)
Openess	Open	Open	Open	Open	Closed
Dynamic membership	Yes	Yes	Yes	Yes	Yes
Lifetime	Transient/ permanent	Transient/ permanent	Transient	Transient	Transient
Surrogate join/leave	No	No	NA	No	Yes
Anonymity					
Sender knows members?	No	No	Yes	Yes	Yes
Member knows members?	No	No	No	No	Yes

Table 3.2.: Brief comparison of multicast service models

[10] The following abbreviations are used: MP–to–MP = Multipoint-to-multipoint, NA = Not Applicable, P–to–MP = Point-to-multipoint, RG = Receiver group, S = Source

4. Framework for the Design of Multicast-Based Mobility Support

Regarding multicast-based mobility support two separate issues need to be distinguished carefully. The first issue deals with the question: A) *'How can a multicast service be provided for mobile hosts?'*. The second issue raises the question: B) *'How can a multicast service be utilized for mobility support?'*. Both questions are closely related to each other: If multicast could be used as a sole mechanism for mobility support (and all applications would use multicast for data transport), then both issues would be identical. Unfortunately, this is not the case due to the problems of the classical IP multicast with mobile hosts. Therefore, there exist two main directions of research. One direction aims at the support of multicast services with unicast-based mobility approaches (such as Mobile IP). The other direction of research intends to modify or augment multicast to support host mobility. The technical problems that arise from question A have been already described in Sect. 3.2.1 and is mentioned for completeness only. The focus of this thesis is rather on question B.

Before considering technical details, the general idea behind multicast-based mobility support can intuitively be described by using the terms introduced in the previous chapter about multicast fundamentals. In general, multicast-based host mobility attempts to utilize mechanisms for data distribution to certain locations, whereas the locations are identified by access points. In principle, one multicast group is created per mobile host. A mobile host can subscribe to a multicast group at its current location – the access point with which the mobile host is currently associated with – or at multiple locations. In the latter case, the mobile host has connectivity to more than one access points or the mobile host has been pre-registered. Data are distributed by multicast in the downlink direction towards the mobile host (Fig. 4.1). Optionally, multicast can also be used to transport data packets uplink originating from the mobile host. Hence, in a wireless network with a mobile host and multiple access points creating cell clusters of neighboring cells data can be efficiently forwarded to multiple access points simultaneously. When a mobile host moves to a new wireless cell that belongs to the cell cluster, the data destined for the mobile host are already available in the access point. The new access point can immediately start forwarding data over the wireless link to the mobile host. Consequently, the service interruption is shortened. The predictive handover is an obvious benefit of utilizing multicast for support of host mobility.

In the design of a solution for multicast-based mobility support a considerable freedom exists in choosing options regarding the network architecture and protocols. In order to classify and potentially extend existing solutions as well as to identify new solutions a common framework for the design of multicast-based mobility support is developed. This framework consists of three parts: requirements, protocol options, and functionalities. The requirements form the basis and goal for designing a particular scheme and judging the merits of existing schemes. Many requirements are evident for mobility support in general. However, a number of requirements include specific conditions for multicast-based mobility support. Based on the requirement analysis protocol options and functionalities for multicast-based mobility support are elaborated. The protocol options reflect particular assumptions regarding network architecture and protocols. The mobility support functions are classified into several categories, each category provides options on the mobility support

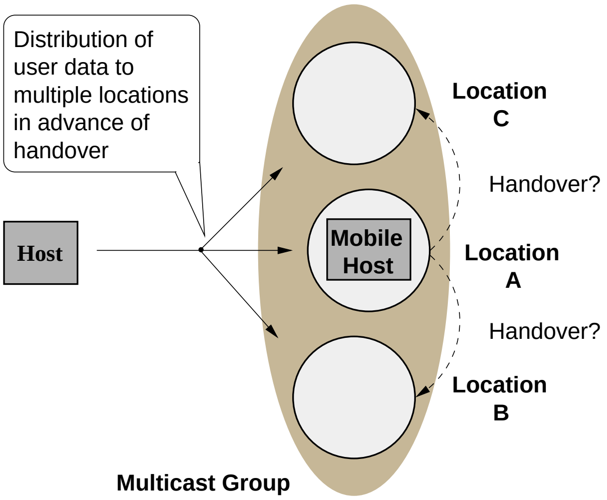


Figure 4.1.: Intuitive understanding of multicast-based mobility

function is executed.

The three components — requirements, protocol options and mobility support functionalities — create a decision space for design. Each combination of options provides a basis for constructing a variant for a multicast-based mobility approach (Fig. 4.2). It will be shown, that existing approaches for multicast-based mobility support can be captured and classified within this framework. The framework will be used to derive candidate approaches that will be investigated as case studies in the following parts of the thesis.

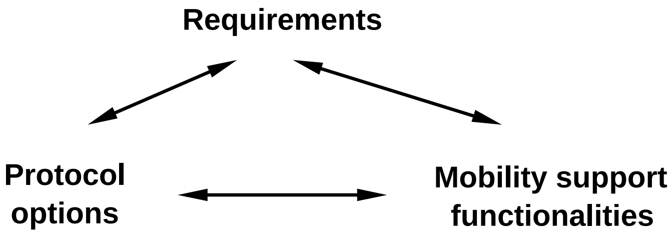


Figure 4.2.: Interdependence of requirements, protocol options and mobility functionalities

The chapter is structured as follows. First, the requirements for multicast-based mobility support are analyzed. Then, protocol options and mobility support functionalities are categorized. Section 4.5 describes how the existing approaches to multicast-based mobility support can be captured with the developed framework. Finally, candidates for multicast-based mobility support are derived in Sect. 4.6. The candidates extend existing approaches or represent new approaches for multicast-based mobility support and will be evaluated in the following chapters of the thesis.

4.1. Requirements of Multicast-Based Mobility Support

Identifying the requirements of mobility support is essential for selecting appropriate functionalities and for choosing among protocol options. In general, the requirements for unicast-based mobility support described in Sect. 2.4 can be adopted for multicast-based schemes. Nevertheless, many of them inhere multicast-specific aspects. Therefore, the requirements from Sect. 2.4 are re-iterated and consequences for the design of a multicast-based mobility solution are emphasized.

Short handover latency and small packet loss. Handovers with short latency and small packet loss require a fast execution of multicast join operations. Multicast management protocols are optimized to reduce the signaling overhead at the expense of increased join latency in order to support large groups of receivers.[1] Unmodified multicast protocols would — in the case of handover — indeed ensure that a mobile host re-joins the multicast group from its new access router, but this would only happen using the slow membership query/report process. Hence, explicit, unsolicited re-join operations are required.

Heterogeneous end systems and access networks. A multicast scheme must cope with different end systems (palm-sized devices up to workstations) and changing access network parameters during a multicast session.

Inter-operation among different multicast schemes. While IGMPv2/v3 and Multicast Listener Discovery MLD [25, 44, 55] provide the access of hosts to most of the IP multicast variants, *proprietary* future multicast schemes may not be compatible with this protocol. A mobile host needs minimal knowledge about the used multicast scheme in order to adapt to the provided multicast protocol.

Scalability Using multicast for host mobility implies a unique multicast group per mobile. Hence, mobile systems supplying potentially a very high number of mobile hosts require a multicast scheme which scales with the number of multicast groups with typically only a few members. Today's IP multicast is designed for scalability with the number of hosts per multicast group and more aspects like the availability of multicast addresses, address assignment, multicast router states, signaling overhead and route aggregation must be taken into account.

Reliable transport of data. A full-scale communication network requires reliable services. In non-mobile IP networks TCP is usually used for reliable data transport. The traditional IP multicast offers an unreliable service based on using UDP. The main reason that prevents the usage of TCP as a reliable transport protocol for multicast is feedback implosion from multiple receivers to a single sender. This feedback implosion would also pertain to an IP multicast-based mobility scheme. Hence, either a multicast-specific reliable transport protocol is required or the multicast must be organized in such a way that allows using TCP between a single sender-receiver pair. Assuming that the mobile host is the only receiver in the multicast group, then TCP might be used.

Location privacy and anonymity. Using multicast for mobility support could potentially provide natural solutions to this problem by the very fact that they separate identity and location, potentially in a fashion that is not noticeable for other end users.

[1] For example, IGMP and MLD defer sending the host's membership report by a random delay. This mechanism reduces the signaling load since usually only a single host sends the report and membership reports of other hosts belonging to the same group are suppressed.

Small signaling overhead. A multicast-based mobility solution utilizes the signaling operations of multicast management and routing protocols, such as IGMP and DVMRP. It must be considered that the multicast signaling messages are sent via a wireless link although these protocols are not adapted to the the limited bandwidth of the wireless link. Most IP multicast routing protocols provide soft state maintenance where the routing state needs to be refreshed and expires otherwise. Hard state maintenance reduces the signaling overhead, but is less robust for stale states which are likely to occur in error-prone wireless and mobile environments.

Small data overhead. Three reasons for data overhead specific to multicast-based mobility support exist. First, redundant packet transmissions can be caused by delays in maintaining the multicast tree (branches not being removed immediately). Evidently, this delay should be kept low resulting in a small data overhead. Second, *broadcast–and–prune* multicast routing protocols employ a data-driven approach for the multicast tree establishment and therefore cause data overhead on network links which do not belong to the multicast tree (those branches will be *pruned* back). Third, a delayed unsubscribe operation results in the transmission of data on links which are about to be removed from the multicast tree. For example, IGMPv1 does not support explicit IGMP leave operations. Hence, the host waits until the next IGMP membership query cycle to implicitly leave the multicast group.

Support of different handover policies. Utilizing the multicast for distribute data to neighboring access points in advance of handover incurs a high protocol overhead in terms of bandwidth and buffer space. In particular the fact, that not all applications have very stringent timing and packet loss requirements results in a demand for handover policies that make a tradeoff between protocol overhead and handover quality. A network should be able to employ these handover policies in a flexible manner.

Assuming that it is possible to construct a single solution that supports all of the above requirements, such a system would provide strong and expensive guarantees even to data flows/applications that do not require them. For example, handover with very small handover latency for web browsing would incur overhead and hence cost that is only necessary for real-time data flows. Therefore, some adaptivity within a single mechanism or an adaptable choice from among a number of mechanisms will be a more economical and equally satisfying solution.

4.2. Protocol Options for Multicast-Based Mobility Support

Multicast protocols can be used in a number of different ways in order to support mobility. The main alternative options are the following:

Communication Environment. Can be either a connection-less or a connection-oriented environment. This option restricts the selection of the multicast type.

Micro- vs. macro-mobility. Using multicast for macro-mobility allows a uniform solution but requires global scalability of the multicast scheme. If, on the other hand, multicast is only used for micro-mobility, an additional solution for migration between access networks is necessary but the scalability requirements are reduced. However, coupling two different mobility solutions will necessitate some form of address translating (between unicast and multicast), e.g. performed in a gateway between access network and Internet. A multicast-based micro-mobility scheme does not need to be scalable to the global Internet which is a requirement for a multicast-based scheme for both macro- and micro-mobility.

Multicast type. Refers to the protocol layer of the used multicast. Main options are network-layer (including IP multicast and unicast-based solutions) and link-layer multicast (especially, ATM multicast). The multicast type determines the service model.

Multicast service model. Describes the services offered by the multicast without specifying how these service are provided. Main options are the any-source multicast (ASM), single-source multicast (SSM), and explicit multicast (XCast) service model in IP networks, the multicast service model of ATM, MCall, etc. as defined in Chapt. 3.

X+Multicast. Multicast based on location-independent addressing and routing can be applied as a sole mechanism for mobility support, but not all multicast schemes enjoy this property (e.g. SGM [19]). Nevertheless, these schemes can be utilized to augment other mobility approaches by specific functionalities. For example, SGM in combination with Mobile IP can be utilized to distribute packets to multiple Mobile IP foreign agents. This case can be expressed by *Mobile IP + SGM*, whereas *Mobile IP* replaces the X.

Multicast endpoint. Selecting the mobile host as multicast endpoint requires multicast protocols to work across the wireless link. This requires multicast protocols which are optimized for efficient usage of the scarce wireless resources and adapted to an error-prone wireless link. Alternatively, the access point might be selected as the multicast endpoint. In this case the access point can act as a multicast proxy and perform multicast signaling operations on behalf of the mobile host. The latter option facilitates the usage of optimized signaling protocols on the wireless link.

Multicast tree directionality. A multicast scheme can provide either unidirectional or bidirectional trees. An unidirectional tree is set up to transport downlink packets from a correspondent host/gateway as the root of the tree towards the mobile host while uplink packets use unicast. With a bidirectional multicast tree traffic is carried on the tree for both up- and downlink.

Dynamic tree. The multicast tree can be static or dynamic. In the first case the access points belong to a pre-established multicast tree and cover a geographical area. The tree is not modified as long as the mobile host remains within this coverage. In the second case, the tree follows the current location (i.e. footprint) of the mobile host.

Multicast adaptation. Existing multicast protocols can be used *as is*, without modifications. However, the protocols might be adapted to better meet the requirements of mobility support.

4.3. Functionalities for Multicast-Based Mobility Support

The functionalities associated with mobility support can be classified into several categories, each provides a basis for constructing a variant for a multicast-based mobility protocol (Fig. 4.3).

Detection of link availability. Access points may advertise their availability on their local links. Assuming the multicast endpoint in the mobile host, a multicast management protocol may provide this functionality (e.g. IGMP membership query/report scheme). Optionally, a mobile host may also solicit advertisements from access points. Corresponding to the IGMP membership query/report scheme, a mobile host may send an IGMP unsolicited membership report. Alternative schemes to advertisements are polling and monitoring. Polling relies on periodic poll messages sent by the mobile host to the access point. Monitoring employs a lower-level protocol to detect another link with better transmission and reception quality.

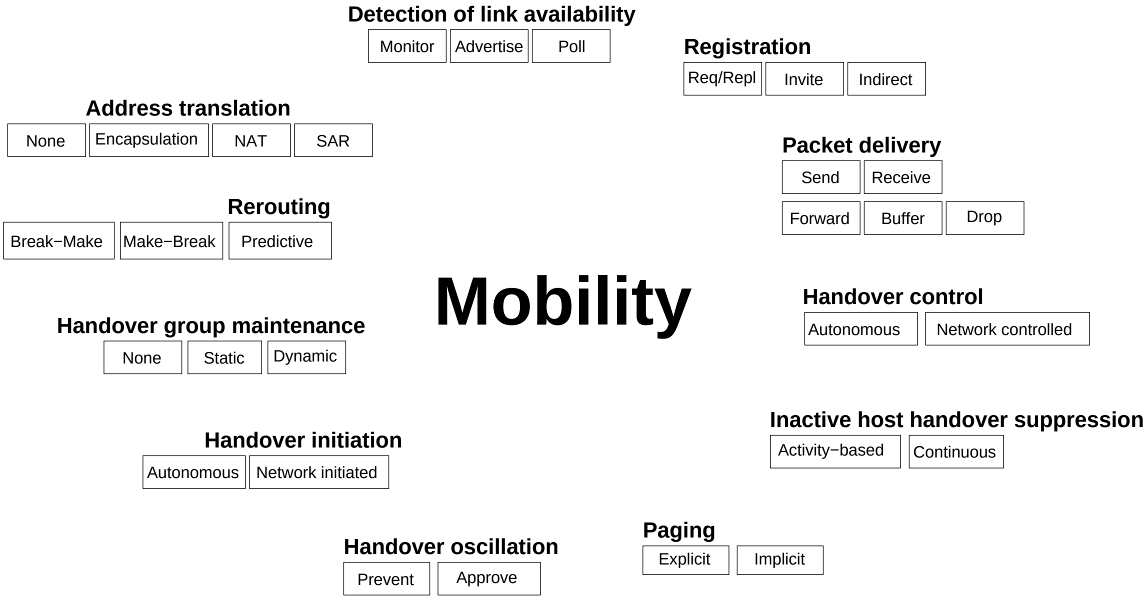


Figure 4.3.: Functional categories for mobility support.

Registration. On top of an existing link-layer connectivity a mobile host registers to update its current location information, enabling tracking. Registration can be based on a request/reply scheme initiated by the mobile host or on an invitation by the access point. Alternatively, a mobile host can also be registered indirectly by another access point. In this case the other access point acts as a proxy and performs the registration on behalf of the mobile host. Assuming that a mobile host is uniquely identified by a multicast address, the subscription to a multicast group using a multicast management protocol represents an implicit registration.

Address translation. Due to the different type of unicast and multicast addresses an address translation might be necessary when a multicast-based micro-mobility approach complements a unicast-based scheme for macro-mobility. This functionality is usually performed in a gateway interconnecting the access network with the Internet and also in the mobile host/access points to reverse the translation. Address translation works either by NAT [149], by encapsulation [128], or Segmentation And Reassembling (SAR).

Packet delivery. Evidently, the basic functionalities are *send* and *receive* in the mobile host and access point. In addition, during a handover packets destined for a mobile host can be sent/received either via the old or the new access point. If packets arrive at an access point that has already lost connectivity with the mobile host, these packets are *dropped*, *buffered* or *forwarded*. When packets are dropped, they can be retransmitted by higher layer protocols if required. Forwarding refers to the functionality that packets are forwarded from the old access point to new access points. This saves retransmission of packets at higher protocol layers. In the buffering strategy, packets are distributed in advance of handover to a set of access points. This saves bandwidth at the expense of buffer space and additional processing for a deferred delivery.

Handover initiation. The handover initiation functionality manages the information about available access points, including advertisement lifetimes and optionally lower-layer protocol information. The handover can be initiated by the mobile host autonomously or by the network based on the knowledge about the wireless connectivity of a mobile host. Evidently, multicast protocols have no notion of handover, but may initiate multicast subscribe/unsubscribe operations implicitly by query the membership. To avoid long handover latencies the mobile mode might be forced to re-join the group.

Handover control. After a handover is initiated, the handover execution can be controlled by the mobile host autonomously or by the network. This includes the control of the sequence of certain multicast operations which are used by functionalities like handover initiation, rerouting and others. A network controlled handover usually requires assistance of the mobile host e.g. by sending measurement reports to the access point. With respect to multicast to control a handover means orchestrating the sequence of multicast group manipulation functions. A related issue is the prevention of handover oscillation (being handed back and forth between two access points).

Rerouting. A rerouting operation changes the network path of packets for a mobile host in a certain network node. A rerouting operation is based on adding and pruning branches of an existing multicast tree and is executed in that network node where the old and the new path to the mobile host diverge. The appropriate multicast operations can be executed in a *break-make* and *make-break* order: new branches are added before old ones are deleted or vice-versa. Additionally, branches can be added to a multicast tree in advance, implementing predictive handover.

Handover oscillation. Handover oscillation causes a mobile host from being constantly handed over when it is simultaneously reachable by multiple access points and thus causes multicast group membership changes. Oscillation prevention prohibits multiple handovers between the same set of access points within a certain duration of time. Oscillation approval provides frequent handover for systems that aim at optimal signal quality.

Inactive handover suppression. A mobile host which does not send or receive for a certain duration goes into an inactive state. For an inactive mobile host the handover initiation is suppressed even if it has moved out of the coverage of the current access point. Hence, the mobile host re-registers less often in order to reduce signaling load on the wireless link. In addition to that, the multicast tree for the inactive mobile host might be released and therefore the number of active multicast groups in the mobile system is reduced considerably.

Paging. Inactive mobile hosts reduce their frequency of handover registration and location updates, saving wireless resources and potentially also allowing release of multicast groups. Paging locates such mobile hosts and multicast can be used to efficiently distribute paging requests to a paging area identified by a multicast group. Paging can be done explicitly by sending paging requests to the access points in the paging area or implicitly when data packets are distributed to access points of the paging area.

Handover group maintenance. A handover group refers to a group of access points providing neighboring or overlapping spatial coverage of cells. A handover group is used for predictive handover. The membership to a handover group can be static or dynamic. In the former case the membership to a handover group does not change, while in the latter case the access points can dynamically subscribe or unsubscribe to handover groups.

4.4. Review of Existing Approaches to Multicast-Based Mobility Support in IP Networks

At the beginning of this chapter two basic questions were asked regarding multicast-based mobility support. At first, the two main approaches are described that answers the question A) for the provision of multicast services for mobile hosts. Then, the existing approaches concerning the utilization of a multicast service for mobility support are described.

4.4.1. Provisioning of Multicast Services for Mobile Hosts

In order to provide multicast services to mobile hosts the current Mobile IP solution [129] proposes *remote subscription* and *bidirectional tunneled multicast*. Both methods provide basic multicast service but do not address new problems that arise when multicast services are extended to mobile hosts.

Mobile IP remote subscription. With this option a multicast router in the foreign networks is required and the mobile host subscribes to the multicast group using it's CoA. When the mobile host performs a handover to a new Mobile IP foreign agent, it has to join the multicast group. If the mobile host is highly mobile, packets will be lost owing to the set-up time associated with the multicast join operation.

Mobile IP bi-directional tunneled multicast. With bi-directional tunneled multicast the Mobile IP home agent must also be a multicast router. Applying this method, the mobile host uses it's home address to subscribe to the multicast group through the home agent. When the mobile host is away from its home network, a bi-directional tunnel between the home agent and the foreign agent is established and multicast packets are sent and received through the tunnel. One disadvantage in comparison with the *remote subscription* method is the fact that if multiple mobile hosts belong to the same multicast address then copies of the multicast packets will arrive at the foreign agent and the mobile hosts receive duplications. Furthermore, packets need to be encapsulated twice: First, the home agent must encapsulate the multicast packet into a unicast packet destined for the mobile host. This is needed to ensure that the foreign agent is able to process the packet since it will not recognize the multicast address. Once the packet is unicast encapsulated, it must be encapsulated again and addressed to the care-of-address. Packets originated by the mobile host are encapsulated with a unicast IP header carrying the mobile host's home address as the source address. Clearly, multiple encapsulations increases the overhead and might cause fragmentation. Finally, multicast control traffic is sent via the bi-directional tunnel and may potentially traverse long distances in network.

The typical problems of long handover latency for moving multicast receivers or packet loss due to moving multicast sources – as described in Sect. 3.2.1 are not tackled by the multicast mobile IP methods. Hence, this is still a challenging problem. However, solutions for selected issues have been proposed, such as [30, 173, 174]

4.4.2. Utilization of Multicast for Mobility Support

One of the first pioneering steps in utilizing multicast for mobility support has been made by Keeton et al. [97] in 1993. They proposed several alternative algorithms for maintaining network connections used to provide multimedia service in connection-oriented networks with cells of nano-size. Their *multicast-based re-establishment scheme* is based on multicast-operations performed by an access point. They distinguish between a multicast-based algorithm *without hints* and *with hints.* In the former scheme, the mobile host registers with the new access point and informs the new access point of the old access point and of all multicast channels originating or terminating on the mobile host. The new access point sends the list with the multicast channels to the old access point and requests that all data for each channel be forwarded to the new access point. In addition, the new access point requests that it be allowed to forward data from the mobile host through the old access point. Concurrently with the forwarding operation, the new access point multicast joins the existing multicast channel(s) to add itself to the multicast channel. After successful establishment of the new branch, the new access point synchronizes the data arriving at the new branch with the data being drained from the old access point by means of buffering in the new access point. Finally, the old access point leaves the multicast channel triggered from the new access point. In the *multicast-based re-establishment with hints* scheme, the current access point is informed by a potential new access point. The current access point notifies that access point to join all of the mobile host's multicast channels in anticipation of a handover. When a handover occurs, the new access point has already initiated join operations. Finally to complete the handover, the new access point informs the old access point to execute a multicast leave operation.

Acampora et al. [1] propose building a *virtual connection tree* covering access points in a local area. The wireless network is split into areas called *neighboring wireless access regions.* In each region, a single fixed switching node acts as the root of the tree. The tree consists of pre-established virtual circuits from the root of the tree to each access point. All connections to a mobile host pass the root node of its current region. When an ATM cell for a mobile host arrives at the root node, it uses the information about the mobile host's location to forward the cell across the appropriate branch of the virtual circuit tree. This delivers the cells to the access points currently serving the mobile host. When a mobile host wishes to route packets through another access point in the virtual tree, it transmits its ATM cells using the virtual connection identifier that has been pre-assigned for communication between the mobile host and that particular access point. When the root node receives these cells, the root node recognizes that a handover has occurred since cells have arrived with a different virtual circuit identifier. Finally, the root node activates the new branch of the virtual circuit tree. When a mobile host changes its region, the network must build an entirely new virtual circuit tree. The approach attempts to reduce signaling overhead caused by handover.

Ghai et al. [66] present an architecture for a pico-cellular network and a multicast-based, connection-oriented communication protocol for seamless mobility support. The authors divide the wireless network into regions controlled by a server host. Hence, the architecture consists of a three-level hierarchy: The *server host* at the highest level tracks mobile hosts and maintains their connections. The *mobile support stations* at the second level provide a wireless cell and act as a connection point for *mobile hosts* at the lowest hierarchical level. The basic concept in the proposal is the *group* that consists of a set of surrounding wireless cells. When a message needs to be delivered to the current group of the mobile host, the server host multicasts the message to the current group of the mobile host. The group is updated each time the mobile host moves between cells. A mobile support station buffers all messages for a mobile host that it receives from the server host. If the mobile host is local, the mobile support station transmits the messages to the mobile host. If the mobile host is not local, the mobile support station holds the messages until either the mobile host enters the cell or the server host sends information that the mobile support station is no longer in the group. In the latter case, the messages are discarded.

Mysore et al. [115, 116] proposed a new kind of architecture for supporting host mobility using IP multicast as a sole mechanism for routing packets to mobile hosts. In their approach, each mobile host is assigned a unique IP multicast address. Packets sent to the mobile host are destined to that multicast address and routed through the network of multicast routers to the host. For locating a mobile host by its IP multicast address, the wireless network is divided into *domains*, where each domain is served by a location server. Each location server is assigned a certain space of multicast addresses. When a correspondent host wishes to communicate with a mobile host, the correspondent host sends a multicast packet to the multicast router in its subnet. The multicast router in turn discovers the location server corresponding to the mobile host and retrieves the address of a multicast router which can forward the packets to the mobile host and joins that multicast distribution tree. As a result of using multicast for supporting host mobility, advance registration and delivery of packets to the next cell in advance of handover is proposed. However, the authors state that a number of factors prevent the deployment of IP multicast infrastructure for mobility support as-is. They identify some of the problems and conclude that additional efforts are needed.

Acharya et al. [2] address the problem of reliable delivery of multicast messages to mobile hosts. They argue that a mobile host may receive more than one copy of the message[2] since the mobile host connects to the network at different times. This is due to the fact that the access points[3] receive the multicast message at different times, or the mobile host receives the multicast message at different times due to latencies within the wireless cells. In the proposed framework, a two-tier protocol architecture is assumed where the access points are responsible for executing multicast protocols on behalf of the mobile host. The authors make use of a *host group* concept. Instead of individually tracking each mobile host, a set of mobile hosts is aggregated into a host group located within a set of wireless cells. The host group is identified by a single multicast group identifier and a Host View Membership Protocol (HVMP) is used for multicast management. A copy of a multicast message is sent to each access point belonging to the host group. Three schemes with different message delivery semantics have been proposed: A mobile host may receive a copy from *at-least one* cell, or from *at-most one*, or at *exactly one* cell. All three schemes rely on a mechanism in which a mobile host's state is transferred from the previous cell to the current cell during the handover process.

Seshan [145] examines the problem of performing fast handover in cellular data networks with a focus on routing updates and state distributions. He proposes the use of multicast to set up routes in advance of handover and hints, based on information from the cellular network to predict handover, intelligent buffering in access points and state replication to avoid explicit state transfers during handover processing. The design, implementation and evaluation of these techniques are described for connection-oriented and connection-less networks. The former environment is also described in [97]. For connection-less environments Seshan assumes a Mobile IP architecture and proposes a scheme in which a mobile host's Mobile IP home agent encapsulates packets destined for the mobile host in multicast packets sending these packets to multiple foreign agents. One of the foreign agents forwards the packets actively. The other foreign agents buffer the packets and forward them when a handover to this particular foreign agent occurs.

Stemm et al. [23, 150] propose a vertical handover scheme utilizing multicast. In principle, Stemm et al. directly continue the work of Seshan [145] for multicast-based mobility support in connection-less environments. The authors assume a hierarchical network architecture comprised of room-size, building-size and wide-area data networks forming a *Wireless Overlay Network*. Each hierarchical level provides a different service in terms of bandwidth and coverage. The vertical handover scheme allows a mobile host to roam among multiple wireless networks. In principle, the handover scheme is based on Mobile IP, but is enhanced by multicast functionalities. A mobile host may use a multicast IP address as care-of-address. The Mobile IP home agent encapsulates the unicast packets into multicast packets and forwards them to the Mobile IP foreign agents which have joined that multicast group. One of the foreign agents is selected as the *forwarding* access point. It decapsulates the packets sent by the Mobile IP home agent and forwards those packets to the mobile host. The

[2] Or it may not receive the message at all.

[3] Mobile Support Stations (MSS) within the context of this work.

other foreign agents buffer the packets. When the mobile host executes a handover, it notifies the current access point to move from forwarding to buffering mode and the new access point to move from buffering to forwarding mode. A *downward vertical handover*[4] is initiated when the mobile host does not receive several foreign agent advertisements. To instruct the old overlay network that the mobile host has switched to the new layer, the mobile host sends a request via the new access point to the old access point. An *upward vertical handover* is initiated when the mobile host is associated with the overlay network and receives several beacons from an other network interface. However, the scheme requires changes in Mobile IP: Both, the home and foreign agent must be enabled to handle multicast addresses as care-of-addresses. Furthermore, the foreign agents must be able to forward requests to other foreign agents.

Xylomenos et al. [175, 176] argue that IGMP is designed for high-bandwidth broadcast LANs. In wireless networks with limited bandwidth and processing power and point-to-point connectivity the soft-state mechanism of IGMP burdens a considerable signaling load on to the mobile host. Instead, they propose an explicit, acknowledged join/leave protocol.

Wu et al. [171] propose a network architecture with Mobility Supporting Agent (MSA) running in access points. The architecture aims at the support of seamless receiver mobility in IP networks and also at reducing the potential packet loss caused by handover. A set of protocols has been designed for the architecture that performs agent discovery and pre-registration. In the architecture the mobility-supporting agents perform multicast operations on behalf of the mobile host. The authors argue that handover latency can be reduced, since the new mobility-supporting agent can send an unsolicited IGMP membership report and does not have to wait for an IGMP membership query cycle which contributes significantly to the overall handover latency.

Mihailovic et al. [108, 109] propose the use of multicast for micro-mobility in an IP access network. For macro-mobility Mobile IP is applied. Hence, their network model consists of two parts: an access network and an Internet-like wide area network interconnected by a gateway. The gateway acts as a Mobile IP foreign agent. The mobile host gets assigned a unicast and a multicast care-of-address for macro and for micro-mobility, respectively. In the access network multicast routers use IGMPv2 and CBT for multicast routing and management, respectively. For communication between a correspondent host and a mobile host the correspondent host sends a packet to the mobile host's home address. The home agent tunnels the packet to the foreign agent in the gateway where the packet is decapsulated and after that encapsulated again in a multicast packet. When a handover occurs where the mobile host remains within the access network the mobile host joins the multicast group via the new access point. For pruning the branch via the old access point the IGMP protocol is extended by a specific functionality for leaving a multicast group. This *instruct* message is sent from the mobile host to the old access point to trigger the CBT process of pruning the unused branch.

Helmy [77, 78] evaluates a multicast-based mobility scheme in a wide-area network. In the assumed architecture the mobile host gets assigned an IP multicast address and the correspondent hosts send packets to that multicast group. As the mobile moves to a new location it joins the multicast group through the new access point and prunes the old branch through the old access point. A performance of the approach is evaluated by means of simulations and compared with Mobile IP.

Uzunalioglu et al. [156] propose a handover rerouting algorithm, referred to as *Footprint Handover Rerouting Protocol* for satellite networks. Due to the movement of Low Earth Orbit (LEO) satellites relative to the Earth, ongoing calls are transferred among satellites.

The existing approaches for multicast-based mobility support described above will be classified in the next section.

[4] From smaller cell to the overlay cells

4.5. Classification of Existing Solutions for Multicast-Based Mobility Support

The framework allows to put together a mobility concept as a combination of certain multicast options and supporting functionalities. Considering each protocol option as a vector, these vectors span a certain vector space. Given the number of vectors with 9 and at least a dimension of 2 for each vector, then the number of possible combinations are $2^9 = 512$. Within this vector space, a number of combinations have already been investigated. Some combinations might be impossible or even not useful. In addition to the protocol options, the mobility support functionalities extend the design options even more.

In Tab. 4.1 is shown how the existing solutions for multicast-based mobility support can be captured with the framework. For comparison the criteria developed in Sect. 4.2 are used.[5] Considering this table in detail, the following conclusions can be made:

- The majority of existing approaches can be classified into two categories: The approaches of the first category attempt to use link-layer multicast in a connection-oriented environment (Acampora [1], Ghai [66]). The approaches of the second category utilize IP multicast in a connection-less environment (Mysore et al. [116], Seshan et al. [145], Stemm et al. [150], Wu et al. [171], Mihailovic et al. [109], Helmy [77]). The latter approaches use the ASM service model of IP.
- While the usage of link-layer multicast for micro-mobility support is considered by Acampora et al. [1] and Ghai et al. [66], link-layer multicast is not an option for macro-mobility. This is due to the fact that link-layer multicast is based on technologies, such as ATM, that has found only limited deployment. Hence, the usage of link-layer multicast is restricted to access networks.
- Most of the mobility approaches, both connection-oriented and connection-less, employ unidirectional multicast trees. This is a consequence of the applied multicast service model, such as the ATM multicast service model or the ASM service model of IP. However, bidirectional trees are not always required and non-multicast transport of data can be used for the reverse direction. A multicast tree is particularly useful in the downlink direction towards the mobile host in order to track the mobile host's movement.
- The majority of the approaches assume a dynamic multicast tree and minimize the number of branches in the tree. Acampora et al. use a static multicast tree with a relatively large spatial coverage and minimize the signaling overhead for reconfiguration of the multicast tree due to handover. However, the approach by Acampora et al. is based on a link-layer multicast and it might be worth considering other multicast types as well.
- Most approaches utilize existing multicast schemes which originally have been designed for multicast in fixed networks. These multicast types do not include mobility-specific functionalities. An alternative option is to design a multicast scheme that better meets the requirements of mobility-support.

Not all of the listed functionalities are provided by the existing approaches. Most of them use multicast without adding mobility-specific functionality and comply them with the functionalities offered by the specific multicast type. The amount of functionalities offered inherently depends

[5] The following abbreviations are used: AP = Access Point, CL = Connection-Less, CO = Connection-Oriented, LL = Link-Layer, MH = Mobile Host , NA = Not Applicable, NWL = Network Layer, SBT = Source-Based Tree

on the multicast type. For example, IP multicast offers inherently a mechanism for re-joining a multicast group by means of IGMP, whereas ATM multicast does not. Other approaches augment the multicast by mobility-specific functionality, such as Wu et al. A third class of approaches uses multicast for a single functionality (e.g. Seshan, Stemm): Efficient distribution of packets to multiple access points. Then, the other mobility-related functionalities are provided by a certain mobility scheme, such as Mobile IP.

Category	Keeton [97]	Acampora [1]	Ghai [66]	Mysore [115, 116]	Acharya [2]	Seshan [145]	Stemm [23, 150]	Wu [171]	Mihailovic [108, 109]	Helmy [77, 78]
Communication environment	CO	CO	CO	CL	CL	CL	CL	CL	CL	CL
Micro vs. macro	NA	Micro	Micro	Macro	Micro	Macro	Macro	Micro	Micro	Macro
Multicast service model	NA	ATM	ATM	ASM	ASM	ASM	ASM	ASM	ASM	ASM
Multicast type	NA	LL Shared	NA Shared	NWL SBT	NWL Shared	NWL SBT	NWL SBT	NWL Shared	NWL Shared	NWL Shared
X+Multicast	NA	No	NA	No	NA	No	No	No	Yes	No
Multicast endpoint	MH	AP	AP	MH	AP	AP	AP	AP	MH	MH
Tree directionality	NA	Uni	Bi	Uni	Uni	Uni	Uni	Uni	Bi	Uni
Dynamic tree	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adaptation	NA	No	NA	No	NA	No	No	No	Yes	No

Table 4.1.: Classification of protocol options for existing approaches to multicast-based mobility support

4.6. Candidate Selections

The framework described in the previous sections allows to identify approaches that are promising candidates for multicast-based mobility support. These candidates are investigated as case studies in the following sections of the thesis. In this section a rationale for the selection of protocol options, in particular of the multicast service models is given.

4.6.1. Justification for the Selection of the Case Studies

The application of the classical ASM service model of the Internet is an evident solution for a case study. It has already been considered in previous proposals, as described in Sect. 4.4: The approach by [115, 116] is based on a *broadcast–and–prune* multicast routing protocol, namely DVMRP. It has to be noted that such *broadcast–and–prune* protocols are optimized to support large groups with sparsely distributed members. This assumption does not match the requirements for mobility support where a multicast tree typically consists of a few branches.[6] A modification of this proposal has been proposed by Wu et al. [171]: Their approach uses explicit join/leave protocols for IP multicast. In general, the first case study derived from the framework follows this latter approach in its basic protocol option choices (e.g. placing the multicast endpoint in the access point) and extend it by additional functionalities (especially support for inactive hosts, paging). In the following, this case study will be termed *MB-ASM*.

Inspecting the first case study MB-ASM using the classical ASM service model reveals that it does not exploit all capabilities of its underlying multicast service model. In particular, the necessary multicast functionalities can also be provided by a simplified service model. One example would be the SSM service model. In fact, for fixed networks a trend to a SSM service model can be identified, particularly driven by the *EXPRESS* [82] proposal and by the availability of a variant of single-source multicast in commercial routers by e.g. Cisco IOS-based routers. Using this reduced service model instead of the full model corresponds to using a source-based tree as the multicast type, resulting in the next candidate, described as case study MB-SSM in Tab. 4.2 and 4.3. The benefits of the SSM service model in comparison to th ASM service model are:

- Less protocol complexity and easy deployment,
- Inhibits denial of service attacks from unwanted sources,
- Averts the problem of address allocation.

In this way, SSM alleviates some of the main problems associated with ASM multicast as a prerequisite for its utilization for host mobility. Moreover, there are other reasons which endorse the usage of SSM: It is ideally suited for tree-like topologies of access networks with a gateway as the root. Since SSM sets up source-based forwarding trees, there is no need for a shared infrastructure with core routers. Finally, the problem of security aggravates in mobile networks and SSM fairly solves the source access control problem by itself. Additionally, it provides the same actual protocol actions as would result from the use of case study MB-ASM. Hence, the handover performance of both these case studies is expected to be practically identical, but the higher efficiency and less overhead results in a better overall performance.

The usage of the MCall service model providing multi-point multi-connection calls motivates the third case study. This service model facilitates advanced functionalities: In contrast to the ASM and SSM service model, the MCall service model facilitates a much better management of the members

[6] The case with a static multicast tree covering a *geographical* area with a very high number of access points is an exception of this rule.

of the multicast group, including the senders, and the communication between them. Particularly, the addition and dropping of end points to and from the call allows the more exact control of rerouting operation, such as break-make and make-break (see Sect. 4.3). Moreover, additional protocol mechanisms such as third-party registration, resource reservation in advance, sub-casting and others are useful and may potentially improve performance. Such mechanisms provide a larger design space and increased possibilities for the design of multicast-based mobility concepts, but are not available in current IP-based multicast protocols. Yet these mechanisms do exist in some multicast protocols for connection-oriented backbones. In order to investigate such mechanisms, the third instantiation of our framework hence uses such a connection-oriented, link-layer type multicast protocol and is summarized in Tab. 4.2 and 4.3 as case study MB-CMAP.

One of the main objections to multicast is the scalability problem. Most IP multicast protocols are optimized to scale with the number of participants per multicast group. However, such an optimization does not reflect the needs of a multicast protocol that is to support mobility: Here, only very few participants belong to a single group, namely either only the mobile host itself or the access points with which the mobile host is currently associated (or immediately neighboring access points in case of predictive handover), depending on where the multicast tree is terminated. But the number of multicast groups is going to be very large. Therefore, a multicast protocol for mobility support should much rather scale with the number of groups, where scalability with the number of group participants is only a secondary concern. Small Group Multicast [20] is a protocol that realizes the XCast service model (described in Sect. 3.2.1). However, this protocol does not separate location and identity and must hence be supplemented by a basic mobility mechanism. Choosing basic or hierarchical Mobile IP results in case study MIP-SGM, whereas basic or hierarchical Mobile IP serves as the underlying mobility scheme and SGM is applied for performance improvement.

4.6.2. Comparison of Protocol Options and Functionalities of the Selected Case Studies

The resulting case studies are *1. MB-ASM using the classical any-source multicast (ASM) service model of IP*, *2. MB-SSM using the single-source multicast (SSM) service model*, *3. MB-CMAP using the multi-point multi-connection call (MCall) service model*, and finally *4. MIP-SGM using the XCast service model in combination with basic and hierarchical Mobile IP*. Tab. 4.2 shows the common protocol options and functionalities for all the case studies and Tab. 4.3 summarizes the differences between the case studies.

Protocol options	
Multicast endpoint	Access point
Dynamic tree	Yes
Adaptation	No
Mobility-support functionality	
Detection of link availability	Advertise/solicit (including link layer trigger)
Handover initiation	Autonomous
Handover control	Autonomous
Handover oscillation	Prevent

Table 4.2.: Basic protocol options (equal values in all case studies)

Considering the common protocol options in Tab. 4.2, it is assumed that the multicast terminates in the access point. Thereby, the mobile host does not need to have any knowledge about multicast.[7] Additional advantages are that this approach better integrates with existing IP-based protocols such as TCP or ARP [115] and that it facilitates the deployment of performance-enabling proxies in the access point improving the protocol performance over wireless links. Other common options are the usage of dynamic trees and the fact that the underlying multicast protocols keep unmodified. The protocol options that are different between the case studies are a consequence of the features of the used multicast service models and protocols. More details will be given in Chapt. 6.

Protocol options	*MB-ASM*	*MB-SSM*	*MB-CMAP*	*MIP-SGM*
Communication Environment	CL	CL	CO	CL
Micro vs. macro	Micro	Micro	Micro	Micro/Macro
Multicast service model	NWL	NWL	LL	NWL
Multicast type	NWL	NWL	LL	NWL
	Shared	SBT	Shared	NA
X+Multicast	Only MC	Only MC	Only MC	MIP/HMIP
Tree directionality	Uni	Uni	Bi	Uni
Mobility-support functionalities				
Registration	Req/Reply & Indirect	Req/Reply & Indirect	Req/Reply & by surrogate reg.	Req/Reply
Address translation	NAT		SAR	Yes/No
Packet delivery	Send, Receive, Forward, Buffer, Drop			Send, Receive
Rerouting	Make-break, Predictive		Break-make, Make-break, Predictive	Break-make Make-break
Inactive handover suppression	Activity-based			None
Paging	Explicit			None

Table 4.3.: Basic protocol options and mobility functions (different values in the case studies)

4.7. Summary

In this chapter a framework for the design of multicast-based mobility support was developed. The framework consists of three basic components: First, *requirements* represent preconditions for the selection of certain mechanisms. Second, *protocol options* reflect architectural and protocol assumptions and third, *mobility support functionalities* are a collection of mechanisms which are required or useful for mobility support. Each combination of protocol options – if reasonable – creates a particular mobility scheme. In addition, the offered mobility support functionalities exploit or augment the underlying multicast scheme.

Within the framework the existing approaches that were described within this chapter can be captured. The framework has been utilized to derive certain case studies that are the subject of further investigation. The case studies are *1. MB-ASM using the classical ASM service model*, *2. MB-SSM employing the SSM service model*, *3. MB-CMAP using the MCall service model* , and finally *4. MIP-SGM with the XCast service model*.

[7] Additionally, for approaches using IGMP the problem of high handover delay is solved which occurs when the mobile host waits for the next IGMP membership query instead of sending an unsolicited join.

5. Methodology for Evaluation of the Selected Case Studies

In the previous chapters the principles of mobility support and the fundamentals of multicast were introduced. In the foregoing chapter a framework for the design of multicast-based mobility support was developed from which four case studies were derived. In the remaining parts of the thesis these case studies will be evaluated and compared.

For the evaluation of the handover performance a combination of the measurements, simulation, and analysis is used. Fig. 5.1 gives an overview about the methodology. For the selected case studies and the reference case basic and hierarchical Mobile IP a common environment was designed. The evaluation environment consists of a prototype implementation for the case studies MB-ASM, MB-SSM, and MB-CMAP (MOMBASA Software Environment [60]), a simulation model for the case study MIP-SGM (based on extensions for the simulation tool *network simulator (ns)-2* [52]), and a prototype implementation for the reference case basic and hierarchical Mobile IP[1]. In addition to these evaluation tools a set of experiments was designed that facilitates a unified investigation of all cases, in particular a comparison between them.

As will be explained later, the experiments for the case studies MB-ASM and MB-SSM are conducted jointly. The experimental results are validated by means of analysis. In addition, the simulation model for the case study MIP-SGM is validated by the measurement results for basic Mobile IP and hierarchical Mobile IP.

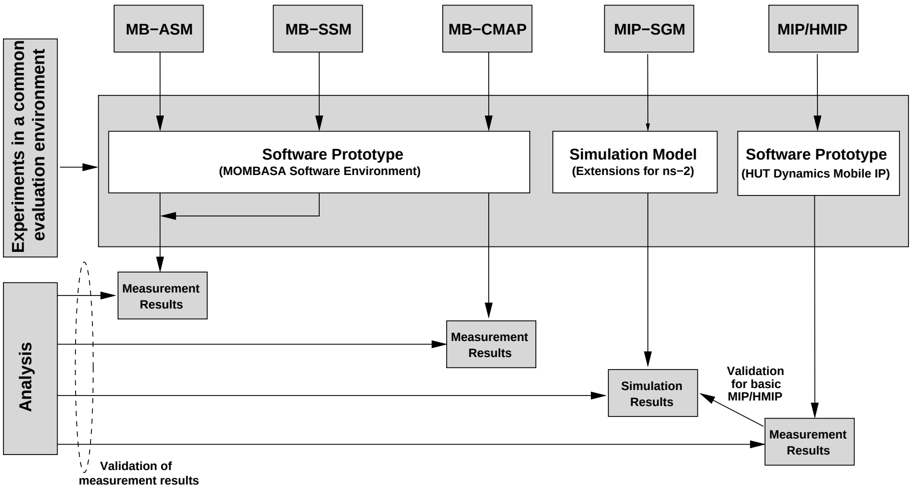


Figure 5.1.: Overview of the methodology for the evaluation of the handover performance

[1] Mobile IP implementation of the Dynamics group at the Helsinki University of Technology [121]

This chapter describes the methods used for quantitative performance evaluation. First, the selection of the evaluation technique is critically discussed. Then, the evaluation process is explained and basic components of the system under study are described. This includes the network model, workload generation, parameterization, as well as monitoring and data collection and statistics. Finally, the measurement and simulation environment for the selected case studies are presented.

5.1. Selection of the Evaluation Technique

In order to evaluate the performance of the selected case studies, a *system*[2] is defined that contains the mobility management schemes as well as the studied wireless communication network. For a quantitative performance evaluation experiments with the system are performed. In principle, these experiments can be done in several ways (see Fig. 5.2). According to Law and Kelton [102], experiments can be conducted with the actual system, or alternatively, with a model of the system. In the latter case a physical model or a mathematical model can be used. While a physical model of a communication network consists of hardware and software which reproduce the actual system in a simplified way, a mathematical model represents a system in terms of logical and quantitative relationships. In both the physical model as well as the mathematical model, certain parameters of the model are manipulated and changed to see, how the model reacts, and thus how the system would react. A mathematical model can further be subdivided into analytical models and simulation models (Fig. 5.2). In an analytical model the system is described by common mathematical expressions or by a formalized analytical method, for example queues or Markov chains [93]. In a simulation model a formalized method, such as a queuing model, is applied similar to an analytical model. However, due to the complexity of the system and of the corresponding simulation model a closed analytical solution is infeasible. The challenge of any model, mathematical as well as physical, is the level of abstraction. The higher the abstraction level, the more low-level details of the system might get lost. Without low-level details the model might not represent the actual system and might generate wrong performance measures.

The corresponding evaluation techniques are analytical modeling, simulation, and measurement, whereas measurements can refer to the actual system as well as to a model of the system. Tab. 5.1, taken from Jain [93], lists criteria for selecting an evaluation technique, whereas the order of items represents their importance. Measurements can only be used if at least a prototype of the studied system exists. For a new scheme without an existing prototype analytical evaluation and simulation are the only techniques. The required time for analytical modeling is usually small, whereas simulation and measurement techniques take more time. The time required for simulation strongly depends on the abstraction level of the simulation model and whether techniques to reduce the time needed for simulation can be applied. An important consideration is the level of accuracy. Analytical evaluation requires a high level of abstraction and often unrealistic assumptions. Simulation can incorporate more details and is regarded to be more realistic. The accuracy of measurements varies; however, a carefully designed measurement can give very accurate, generally valid results. Usually performance evaluation is the basis for selecting a certain alternative among multiple possible schemes. In this respect analytical modeling provides the deepest insight into the impact of parameters on the system's reaction. Simulation offers to vary the parameter space in a large amount, but often it is difficult to clearly present the tradeoff among these parameters. 'The difficulty with measurements is the dependence of the measurement results on the experimental setup that can make the interpretation of the results difficult.' [102]

[2] 'A system is defined to be a collection of entities, e.g. people or machines, that interact together towards the accomplishment of some logical ends.' [143]

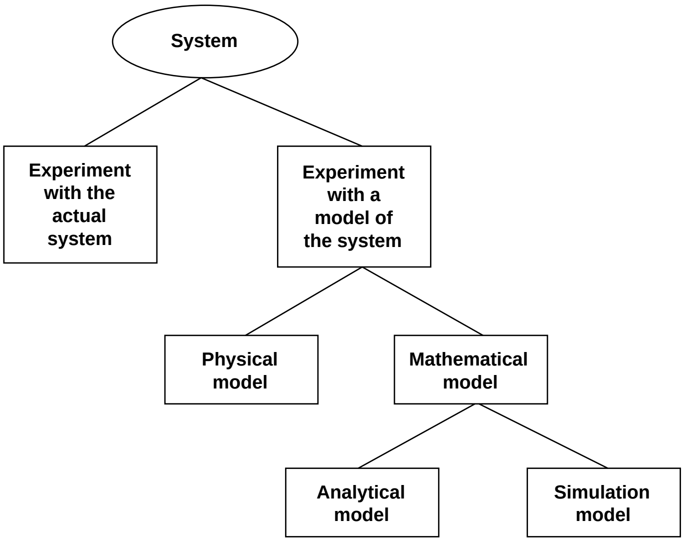

System
Experiment with the actual system
Experiment with a model of the system
Physical model
Mathematical model
Analytical model
Simulation model

Figure 5.2.: Different ways to study a system [102]

Criterion	Analytical Modeling	Simulation	Measurement
1. Stage	Any	Any	Post-prototype
2. Time required	Small	Medium	Varies
3. Tools	Analysts	Computer languages	Instrumentation
4. Accuracy	Low	Moderate	Varies
5. Trade-off evaluation	Easy	Moderate	Difficult
6. Cost	Small	Medium	High
7. Saleability	Low	Medium	High

Table 5.1.: Criteria for selecting an evaluation technique [93]

In this thesis for the quantitative performance evaluation of the mobility schemes, a combination of analytical evaluation and measurement has been selected. For one of the case studies a simulation in place of the measurement is executed; the reason for this exception is explained below. However, the evaluation techniques measurement and analytical modeling are used complementarily instead of exclusively. The combination of measurement and analytical technique is a consequence of the complexity of the investigated system. The combination allows the usage of an evaluation technique when it is most useful. Measurements are applied to investigate mobility-related performance metrics, such as handover latency and packet loss. In order to examine scalability effects an analytical technique is applied where measurements would incur considerable costs for equipment and experimental logistics. For example, increasing the number of mobiles in the experimental setup in order to examine the dependency of the handover latency of the number of mobiles in the network would cause high costs in terms of equipment and time.

A combination of the evaluation technique also allows a validation of the achieved results. In particular, the results from measurements are more vulnerable to experimental errors than the other techniques. Therefore, a validation of the measurement results by analysis ensures correct measurement results. In addition, the prototype may include specific implementations having a strong impact on the measurement result. By using an analytical technique for validation, such measurement errors and falsification can be minimized.

Although multicast-based mobility support is a promising research topic, the general idea of using multicast for mobility support has been investigated in several efforts as described in Sect. 4.4. Most of the existing approaches have used an analytical or simulation technique to prove the usefulness of their approach. Nevertheless, some skepticism towards multicast-based mobility support in the research community could be recognized. In particular, basic mobility schemes like Mobile IP, hierarchical Mobile IP and Cellular IP were implemented as prototypes. Therefore, a need for the development of a prototype for multicast-based mobility support has been identified. Moreover, a lack of appropriate tools for investigation of multicast-based mobility support in the research community exists, in particular for different multicast types. Consequently, a software platform is developed as part of the thesis. The platform consists of a collection of components that is the basis for the prototypes used for the measurements. Further details of the software platform for the multicast-based mobility are described in Chapt. 7. For measurements of the reference case basic and hierarchical Mobile IP an existing prototype was used under comparable experimental conditions.

In comparison to a simulation technique the chosen measurement technique has advantages and also drawbacks. One of the advantages is the fact that a measurement technique involves much more low-level details. Moreover, a measurement technique supersedes the development of an appropriate system abstraction as the simulation model. This modeling phase is a critical phase for simulation since low level details can be lost. A common drawback of measurements are higher costs, in particular of the experimental equipment, but also for developing a prototype of the mobility management schemes as well as conducting the experiments when many factors need to be altered. However, the argument of high costs for equipment is alleviated in this particular case. As it will be described in Chapt. 8 the experimental setup for the case studies MB-ASM and MB-SSM is composed of standard equipment at relatively low costs, in particular the hardware components are based on conventional personal computer and networking equipment. For the third case study MB-CMAP an open, non-proprietary networking equipment for use in experimental systems research was deployed.[3] Considering the duration of time needed to execute the simulation runs, the simulation technique is often regarded as the less time-consuming approach. Nevertheless, a feature of mobility systems has to be taken into account: In such a system handover events usually occur rarely on a time scale of

[3] The equipment is part of the *Washington University's Gigabit Network Technology Distribution Program.*

typically 10^0 to 10^3 seconds. In a real mobile system the time scale of events, such as packet arrivals, is much smaller. For simulation this results either in long simulation runs limiting its practicability *or* in modeling at a higher abstraction level at the expense of accuracy. Although the simulation of rare events can be accelerated by sophisticated methods, such as *RESTART* [158], these methods are still in an early stage of research and have been proven for relatively simple systems.

Whereas the case studies MB-ASM, MB-SSM, and MB-CMAP are examined by measurements, a simulation technique is applied for the fourth case study MIP-SGM. The main reason for this exception is the fact that the developed prototype can not be utilized for this case study due to its basic difference to the cases: MIP-SGM relies on basic and hierarchical Mobile IP as the underlying mobility scheme that is not part of the developed prototype. Contrary to the other case studies a simulation model for this scheme is developed whereas the simulation model is validated with measurement results of the reference case basic and hierarchical Mobile IP.

An overview of the used techniques for evaluation of the case studies is given in Fig. 5.3.

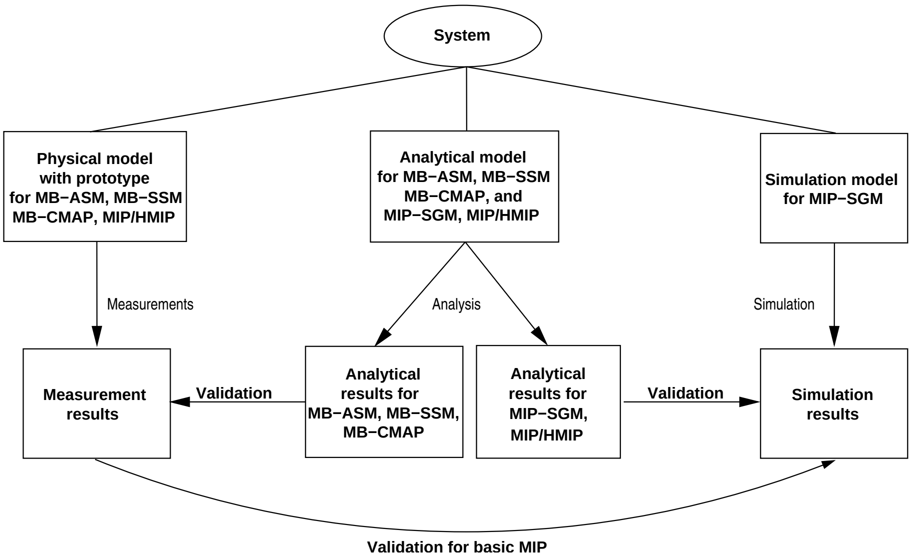


Figure 5.3.: Overview of evaluation techniques for the case studies

Fig. 5.4 illustrates the main process of the measurement technique. Four processes can be distinguished: The workload generation process that inputs data to the modeled communication network executing the mobility management schemes, the process for monitoring and data collection, and finally, the process for evaluation and statistical calculations. The main process is common to both the measurement and simulation technique. Considering a measurement technique it is presumes that the mobility management schemes are implemented at least as a prototype. These schemes operate with a model of the real network that will be realized as an experimental setup. For experimental evaluation of different scenarios and factors, the network model, as well as the prototype implementation are controlled by network configuration parameters. In order to study certain mechanisms with the prototype policies are modified to force the selection of these mechanisms. An important part of the overall system is the load generation. In general, in a mobile network the load generation consists of two models: for traffic generation and for host mobility. In the next sections the network model and the workload model are described. The remaining components of the evaluation process are explained in other chapters of the thesis: The prototype implementation of the mobility schemes and policy selection in Chapt. 7 and measurement statistics in Chapt. 8.

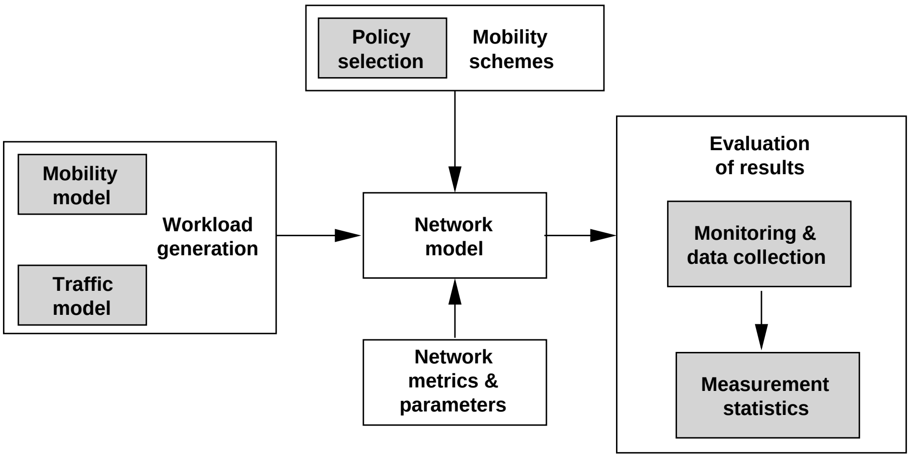


Figure 5.4.: Quantitative evaluation process for measurement and simulation

5.2. Network Model

The following subsections describe the models of the real network with increasing abstraction level: the physical model for measurements, the simulation model, and the analytical model.

5.2.1. Physical Network Model for Measurements

The network model reproduces the real, physical network. The architecture of an IP-based wireless network has been briefly described in Sect. 2.2. Considering the architecture at a high level (see Fig. 5.7), the overall network can be divided into an access network and a Internet-like Wide Area Network (WAN). Several IP networks are attached to the WAN: one network typically represents a network with a host or server corresponding to a mobile host (correspondent host). Another network attached to the WAN stands for the network where a mobile host usually is located. For selected mobility schemes, such as Mobile IP (see Sect. 2.5), this home network plays a decisive role. The networks attached to the WAN representing the Internet are IP networks as defined in Sect. 2.2. The access network is considered as a network in the IP sense (or a compound of multiple IP networks) that can be divided into multiple subnetworks. The size of the access network can range from a small IP network (e.g. class C IP network) or multiple class C networks structured by means of CIDR, up to an AS in an extreme case. The access network also represents an IP routing domain in which the nodes operate common routing protocols. Basic elements of the access network are access points and routers. The access points are interconnected to routers as well as routers among each other. One or more dedicated routers act as gateways interconnecting the access network with the WAN. Typically the topology of the access network is tree-like with a gateway as the root and access points as leaf nodes. It is assumed that each wireless cell creates an IP network or subnetwork and access points act as IP routers. The access points of a single access network may provide different wireless technologies. Each technology provides a certain bandwidth and coverage.

A mobile host is assumed to be located within the service area of the access network. While communicating the mobile host moves within the spatial coverage of the wireless cells. Two scenarios are distinguished: Pico-/micro-cell scenario and pico-cell scenario. While a pico-cell has a diameter of multiple 10 meters, the diameter of a typical micro-cell is multiple 100 meters. In a pico-/micro-cell scenario (Fig. 5.5(a)), pico-cells lie within the spatial coverage of a larger micro-cell. In a pico-cell scenario (Fig. 5.5(b)) multiple pico-cells are grouped into a cell cluster. When a mobile host moves within the spatial coverage of a pico-cell cluster, the mobile host executes horizontal handovers. In a micro-/pico-cell scenario the mobile host executes both horizontal and vertical handover. In reality, other scenarios can be identified as well. For example, it can be expected that in outdoor areas with a small user density wireless networks will be designed to provide large wireless cells (e.g. macro-cells with a diameter of multiple kilometers/miles). Another extreme are so called nano-cells with a diameter of multiple meters. However, the focus of the measurements is on pico-cell and micro-pico-cell scenarios that are expected to be typical in next-generation wireless networks, based on WLANs and UMTS-like networks.

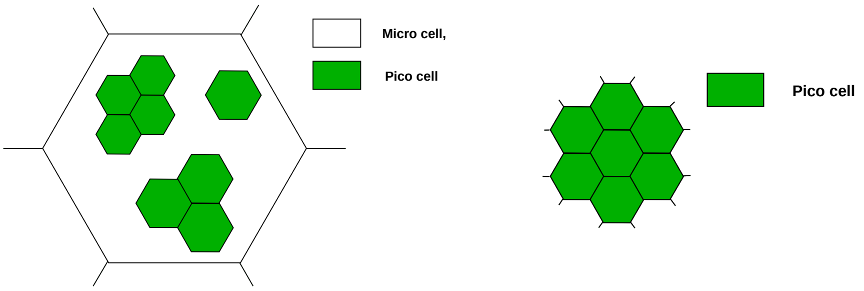
Since it is assumed that the access network consists of multiple IP networks or is divided into subnetworks and each wireless cell represents an IP network/subnetwork with the access point and the mobile hosts, the net-id/subnet-id changes when a mobile host moves to a new cell. Consequently, the mobile host executes an IP-level handover when it changes the cell. This pertains to both handover types described above – horizontal as well as vertical handover.

In a real network communication is not affected by mobility effects only. Typically, a wireless channel is error-prone. High bit error rates varying over time or even link outages are common to a wireless transmission. In addition to the behavior of the wireless links the packet transport in a fixed network is affected by delay and losses, in particular a WAN may generate significant packet delay and packet loss. For example, the typical round-trip time of packets between hosts in Europe and North America using the Internet is more than 100ms.

In Fig. 5.7 the high-level architecture of the network model is faced with the real network. Fig. 5.7 shows the topology of the network model that is used for the measurements. In general, it consists of an access network and a simplified WAN-like network. The access network consists of several network nodes: a mobile host that is interconnected directly with the access points, and two network nodes – one of them interconnecting the access points and one dedicated network node interconnecting the access network with the WAN. In the considered model a single mobile host executes a ping-pong handover between the access points. A ping-pong handover consists of two phases. In the first phase the mobile host is associated with access point A and executes a handover to access point B. In the second phase the mobile host executes a handover from access point B to access point A. This process is executed forth and back, and therefore mobile executes an infinite number of handovers.

In contrast to a real network, the wireless link in the network model for measurements is replaced by a wire-line connection. By this replacement it is possible to abstract from an error-prone wireless channel. For simulation a simulation model of an IEEE 802.11 wireless link is used and the model parameters (e.g. transmission power, etc.) adapted that errors on the wireless link occur rarely. By avoiding errors on the wireless link it is possible to separate the impact of mobility on communication and wireless errors.

The other part of the network model represents the Internet-like WAN. It consists of a correspondent host, a router representing the home network for these mobility schemes that require such a network. The main component is a WAN emulator, a dedicated router that is able to emulate the behavior of WAN links. Effects that can be emulated include packet loss, packet delay, packet miss-ordering, bandwidth limitation and others. However, the main functionality of the WAN emulator as used in the measurements is adding a pre-defined delay to the delay that is caused by the experimental setup.



(a) Pico-/micro-cell scenario

(b) Pico-cell scenario

Figure 5.5.: Two selected scenarios in a wireless network

The architecture shown in Fig. 5.7 represents a topology common to all of the case studies. For each of the case studies a specific setup is derived. In addition to the principles derived above, the setup includes dedicated network components, interfaces to each other, protocol stacks, and others. A detailed description of the measurement setups can be found in Sect. 8.1.

5.2.2. Network Model for Simulation

The simulation model has many similarities with the physical model for measurements (Fig. 5.7(b)) since it is based on the same topology: an access network and a WAN representing the Internet. The access network consists of a single mobile host and two access points that are interconnected by a router. This router acts as a gateway to the WAN. In order to compare the simulation results with measurement results of the other case studies, the network model also contains a dedicated router emulating the WAN behavior. The IP network structure is the same as for the physical network. The access network as well as the WAN network are networks in the IP sense. The access network is can consists of multiple IP network and can be divided into subnets, whereas at least each wireless cell represents an own IP subnet.

The abstraction level of the simulation model is the *packet* level. Basically, the simulation model consists of interconnected queues that can delay and drop packets. In addition to the network of queues, protocol agents (e.g. Mobile IP foreign agents) are executed in the nodes that exchange signaling messages and control the interconnection of the queues. The protocol agents in the simulation model realize a subset of the overall functionality of the real protocol instances.

5.2.3. Network Model for Analysis

This network model is used to analyze the signaling overhead. It further simplifies the real system in comparison to the physical network model for measurements and the network model for simulation. The network model for analysis basically consists of nodes and wireless cells. The nodes execute protocol agents and exchange signaling messages. The simplified topology of the access network consists of gateway, routers, and access points that create a tree topology with the gateway as the root and the access points as the leaf nodes. It is assumed that the gateway and routers have eight interfaces at all – a single upstream interface and seven number of downstream interfaces. This results in a topology best described as a complete and regular tree-like graph.

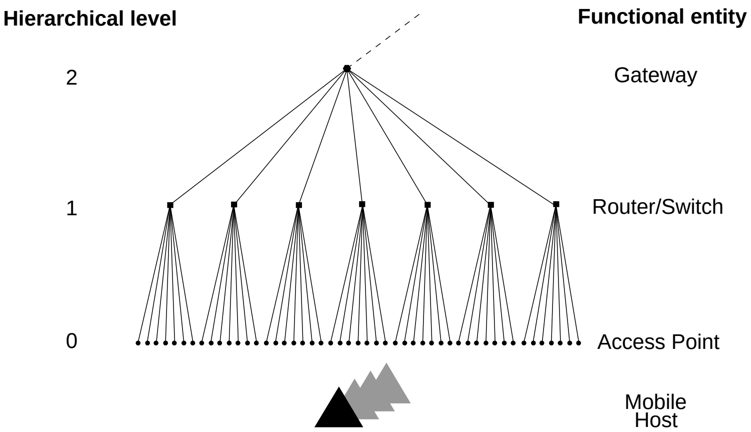
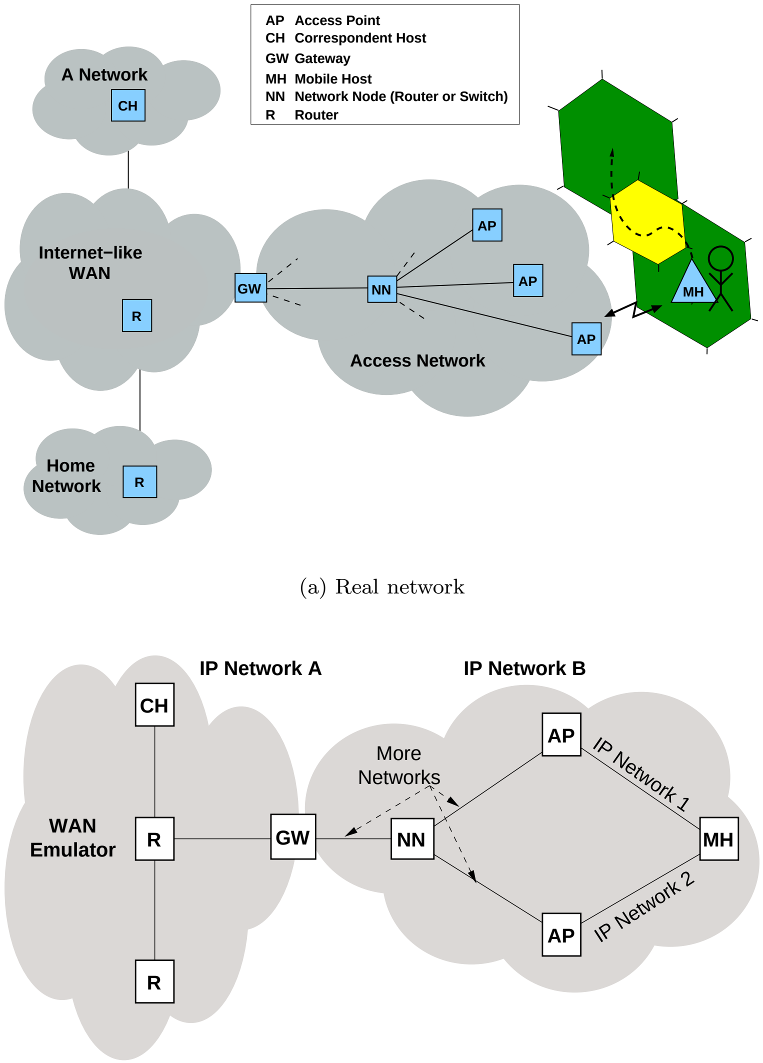


Figure 5.6.: Topology of the network model for analysis

The network model for analysis is based on the same IP structure as the physical and the simulation network model. The access network consists of multiple IP networks whereas at least each wireless cell represents an IP network attached to other networks by means of an access point. The movement of mobile hosts between wireless cells triggers the execution of a network level handover at the IP protocol layer.

An example tree topology with two hierarchical levels is shown in Fig. 5.6. For the analysis of the signaling costs in an access network in Appendix C a network model with three hierarchical levels is applied.



(a) Real network

(b) Network model for measurement and simulation

Figure 5.7.: High-level architecture of the investigated network

5.3. Workload Model

The workload serves as an input to the network model. It consists of two basic components. The mobility model expresses the activity of users mobility. The traffic model describes the data traffic pattern that is generated by the mobile and/or the correspondent host.

5.3.1. Mobility Model

In order to describe the mobility of a user, and respectively that of a mobile host, the term *Cell Dwell Time (CDT)* is used. It indicates the amount of time that a mobile host remains in a cell. The cell dwell time depends on a number of parameters: the velocity of the mobile host, cell size, cell shape, the traversed path, the transmitted power, the signal propagation, as well as interference. To simplify the complex model [15, 18, 84] it is assumed that the cell dwell time is a random variable and exponentially distributed with mean $1/\lambda$. The Probability Distribution Function (PDF) for the cell dwell time is

$$f(t) = 1 - e^{-\lambda t} \quad t \geq 0 \tag{5.1}$$

In Fig. 5.8 the probability distribution function PDF of the cell dwell time for selected values of λ is shown. The mean is assumed to be proportional to the average speed v of the mobile host and inverse proportional to the cell radius R:

$$\lambda = \frac{1}{T} = \eta \frac{v}{R} \tag{5.2}$$

where η is assumed to be constant 1. As an example, a given cell radius $R = 10m$ and a speed $v = 1\frac{m}{s}$ gives $\lambda = 0.1\ s^{-1}$.

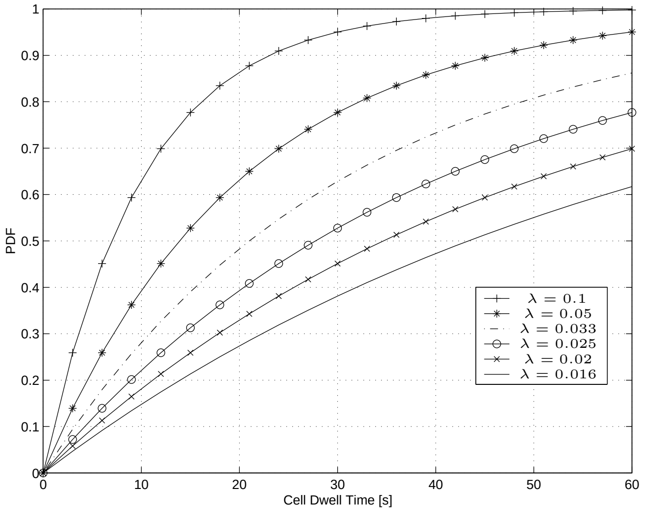


Figure 5.8.: PDF of the cell dwell time for selected values of λ

Moreover, it is assumed that the cell dwell time is independent and identically distributed (IID). Thus, the arrival of handover events can be modeled as a Poisson process with the cell-dwell time as the inter-arrival time between handover events. Then, the number of handover events within a given time interval t can be approximated by the Poisson distribution:

$$p[n, \lambda] = \frac{e^{-\lambda * t} \lambda * t^n}{n!} \qquad n = 0, 1, \ldots \tag{5.3}$$

In Fig. 5.9 the distribution of the number of handover events for a time interval $t = 3600\ sec. = 1\ hour$ with $\lambda = 0.1 sec^{-1}$ is shown. It can be seen that about 90 percent of the samples are between 310 and 410 handovers in the observed time interval of 1 hour.

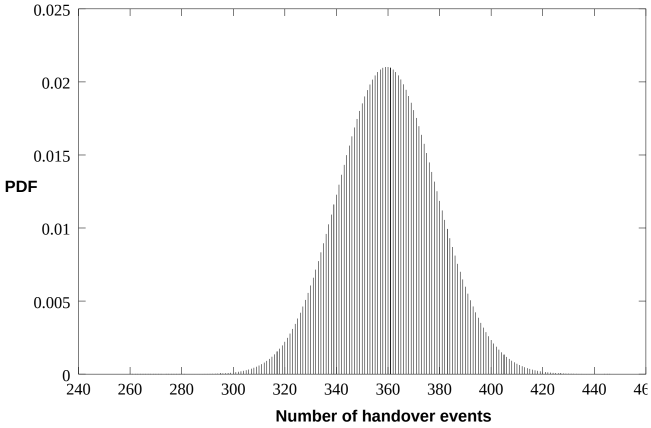


Figure 5.9.: PDF of the number of handover events (time interval of 1 hour, $\lambda = 0.1$)

Subsequent handovers with very low cell dwell times lead to the phenomenon that the mobile host changes the cell without registering with the actual foreign agent. This case occurs when the cell dwell time is smaller than the time needed to trigger a handover (e.g. by means of the lifetime of the last received advertisement). To avoid this situation a constant offset ϵ is added to the cell dwell time. Then, Eq. (5.1) can be written as

$$f(t) = \begin{cases} 0 & 0 \leq t < \epsilon \\ 1 - e^{-\lambda t} + \epsilon & t \geq \epsilon \end{cases} \tag{5.4}$$

The PDF of the cell dwell time with ϵ set to 5 is shown in Fig. 5.10.

It is noted that due to the offset ϵ the handover arrival process loses its memoryless property and can not be modeled as a Poisson process. Therefore, Eq. (5.3) represents only an approximation for the number of handover events in a time interval t of the traffic model.

For the mobility model in the signaling cost analysis it is further assumed that each mobile moves in a purely random fashion. Assuming a hexagonal shape of the wireless cells, the probability of moving to each of the 6 neighboring cells equals $(\frac{1}{6})$. Correlation between successive movements is ignored.

5.3.2. Traffic Model

In order to investigate the impact of handover on the user data, traffic is exchanged between the mobile and the correspondent host. Instead of considering specific applications, such as file transfer or web browsing, the focus is put on the impact of mobility on transport layer protocols. Hence,

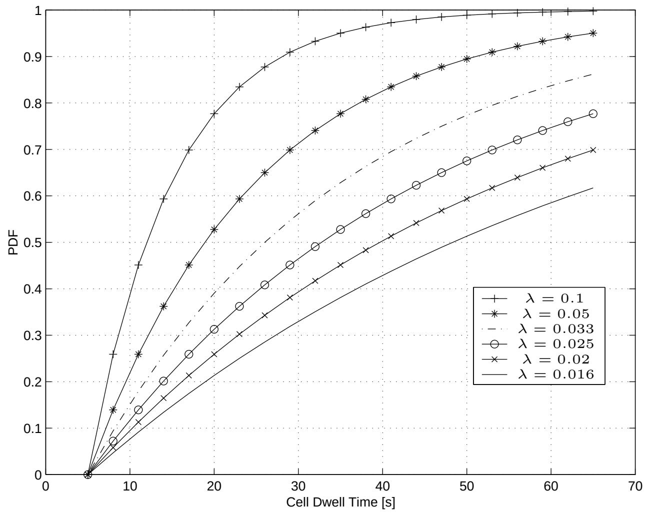


Figure 5.10.: PDF of the cell dwell time with offset $\epsilon = 5$s for selected values of λ

the traffic model describes exchanged transport layer traffic. In principle, the traffic is modeled as a bulk data transfer controlled by several parameters.

Traffic type	Type of bulk data transfer (UDP or TCP).
Packet size	Fixed size of the UDP packet.
Packet burst size	Number of packets sent in a burst.
Inter burst size	Waiting time between subsequent bursts.
Socket buffers size	Size of the socket buffer in mobile host and correspondent host. The socket buffer size determines the size of the TCP advertised window and therefore the maximum segment size in TCP.

The offered load is calculated as follows (for UDP only):

$$\text{Offered load} = \frac{\text{Packet size} * \text{Packet burst size}}{\text{Inter burst size}} \tag{5.5}$$

The offered load is varied by means of changing the inter burst size. The packet size remains constant. The feature to generate bursty traffic (with a packet burst size larger than 1) is unused.

The offered load for TCP traffic is controlled by the TCP flow control mechanisms. Recall that TCP is always bidirectional since TCP data packets are acknowledged by the receiver. Thus, for up-link traffic acknowledgments which are sent down-link must be taken into account.

The traffic model for the signaling costs analysis further simplifies the above model since it is not based on exchanging packets, but instead the communication is regarded as sessions. During a session, the mobile host is active, while after a certain idle-period a mobile can switch to an inactive state. This behavior is modeled as follows: The overall number of mobile hosts in the access network is divided into those that are active and those that are inactive. The proportion of the number of active mobile hosts to the overall number of mobile hosts is indicated by α.

5.4. Evaluation Criteria

This section lists and describes the criteria for evaluation of the case studies and the reference case.

5.4.1. Handover Performance

Handover is a key functionality of a mobile wireless network, in particular in networks with small wireless cells and highly mobile hosts. In order to estimate the handover performance, three metrics are defined: handover latency, UDP packet loss and duplication caused by handover, and TCP throughput. Handover latency is a good indicator to compare the performance of the mobility schemes, whereas the UDP packet loss and duplication and TCP throughput is a better metric for the service quality seen by the application.

Handover Latency

During a handover, the mobile host experiences a certain duration without being able to send and receive data packets. This service interruption is referred to as *handover latency.* It is commonly described as the time it takes a mobile host to resume data traffic after the handover event has occurred.

In order to determine the handover latency precisely, it is worth considering the handover latency in detail. According to [24], the handover latency can be decomposed into two phases: the duration to detect the handover and to execute the handover ($T_{\text{HO\_Detect}}$ and $T_{\text{HO\_Exec}}$)[4] [24]. However, it depends on the handover type as defined in Sect. 2.1, whether the phase contributes to the handover latency. Considering *hard handover*, $T_{\text{HO\_Detect}}$ depends on several issues: *First*, the time it takes for a mobile host to move from the coverage of the old wireless cell to the new cell contributes to $T_{\text{HO\_Detect}}$. This time depends on the spatial coverage (spatial overlap cells, gaps between cells), and therefore strongly on the environmental conditions for wireless propagation. *Second*, the mobile host must associate with the new access point and probably de-associate with the old access point at the link layer. The duration of time for this process is technology-specific. *Third*, in comparison to advertisement-based trigger a link-layer trigger for handover can shorten $T_{\text{HO\_Detect}}$ significantly. How fast a link-layer trigger reacts to the loss/re-establishment of link-layer connectivity depends on the used parameter for link-layer trigger (signal strength, bit error rate, etc.) and again on technology-specific values (such as frequency of link-layer beacons). See e.g. [57] for a discussion of these issues.

With soft handover the mobile host is able to have connectivity to the old and the new access point simultaneously. In the case of overlapping wireless cells the mobile host receives data packets on the link to the old access point until the data path is switched to the link of the new access point. Consequently, for soft handover $T_{\text{HO\_Detect}}$ does not contribute to the handover latency. If the wireless cells do not overlap, the time it takes to move to the new cell until the handover is detected is considered as $T_{\text{HO\_Detect}}$.

With a predictive handover scheme, the new access point forwards buffered data packets to the mobile host as soon as the mobile host has associated with that access point. Therefore, the duration $T_{\text{HO\_Detect}}$ is as large as with the hard handover scheme, and has the same dependencies as described above. In comparison with the hard handover scheme $T_{\text{HO\_Exec}}$ for predictive handover is expected to be shorter since the traffic flow is considered to be resumed when the mobile starts receiving the buffered packets.

For the measurement of the handover latency the following traffic flow model is defined: A continuous traffic flow of packets is received by a mobile host whereas the mobile host executes a handover

[4] Also referred to as *rendezvous time* and *protocol time.*

during the receive process. The handover latency is then defined as the duration from the reception of the last packet before handover via the old access point to the reception of the first packet via the new access point. The granularity of the measure is determined by the inter-packet time of the traffic flow. It is precise for a infinitesimal small inter-packet times. In reality, the granularity is determined by the timer granularity of the operating system and can be regarded as a measurement error.

UDP Packet Loss and Duplication Caused by Handover

The *packet loss* is the number of packets that are lost during the handover process. In general, in wireless and mobile networks packet loss is mostly caused by bit errors in an error-prone wireless channel, congestion in the network, or due to handover. The main reason for packet loss caused by handover is the fact that packets are routed to the old access point while the link to the old access point is already broken. These packets might be dropped by the old access point. In order to estimate the packet loss due to handover, the overall packet loss must be decomposed into the portions by each contributing reason for loss. In this evaluation the following assumptions are made: The wireless channel is assumed to be reliable, and the network nodes operate under low up to medium load. Hence, the other reasons for packet loss than handover (congestion, error prone wireless channel) can be neglected.

The number of lost packets is an indicator for the service quality seen by the application. As described in Sect. 2.4, real-time applications that realize a two way communication require a small end-to-end delay, and therefore, can not retransmit lost packets. Other applications that require a certain degree of reliability, retransmit packets. Retransmissions, in turn, increase the delay and jitter, and consume bandwidth. Additionally, flow control mechanisms triggered by loss reduce the transmission rate of the sender.

The *duplication of packets* has less impact on the application than packet loss. Usually, duplicated packets are dropped at the application layer. However, the number of duplication packets per handover is a measure for the amount of unnecessary usage of bandwidth, in particular of the wireless link.

Impact of Handover on TCP Throughput

TCP is a transport protocol that provides a fully-reliable byte stream service to applications. TCP uses sequence numbers and acknowledgments on an end-to-end basis between hosts. TCP is tuned to perform well in wire-line networks where packet loss occurs mostly due to congestion. TCP responds to losses by invoking its congestion control and avoidance mechanisms, even though the loss might be caused by handover. TCP recovers from packet loss by means of two mechanisms: *retransmission timeout* and *fast recovery.*

A *retransmission timeout* occurs if a sent TCP segment is not acknowledged after a certain duration. TCP interprets the timeout as congestion in the network and retransmits the oldest packet that is not yet acknowledged. TCP waits for the acknowledgment of the retransmission before it continuous, and it gradually increases the number of packets in flight (determined by the congestion window).

The *fast recovery* mechanism allows – as the name indicates – faster recovery from packet loss: When a single packet is lost in a bulk transfer, the TCP receiver returns duplicated acknowledgments to the sender that acknowledge subsequent data packets instead of newly received data packets. The TCP sender receiving the duplicated acknowledgments uses these acknowledgments as an indication that a data packet is lost and retransmits the packets without invoking the *retransmission timeout* mechanism. When the TCP sender has received three duplicate acknowledgements (4 in all), the TCP sender retransmits the lost segment without waiting for timer to expire

Both mechanisms impact the TCP throughput. When the handover latency is larger than the actual *retransmission timer*, the *retransmission timer* mechanism is activated. During the handover latency the TCP sender send TCP segments limited by the congestion window, but does not continue since it does not receive any TCP acknowledgements. Then the TCP sender is idle up to the retransmission timeout. After the retransmission timer has expired, the TCP sender increases its congestion window only gradually. When the handover latency is smaller than the actual *retransmission timer*, the TCP *fast recovery* mechanism is invoked, and the impact of handover on the TCP throughput is expected to be smaller. In general, the TCP throughput is a good indicator to estimate the impact of handover on applications that use TCP as a reliable transport protocol.

In this evaluation the *relative TCP throughput* B_{rel} is defined as

$$B_{\mathrm{rel}} = \frac{B_{\mathrm{TCP,\ w/\ HO}}}{B_{\mathrm{TCP,\ w/o\ HO}}} \tag{5.6}$$

where $B_{TCP,\ w/\ HO}$ is the TCP throughput with handover and $B_{TCP,\ w/o\ HO}$ the TCP throughput without handover.

A degraded throughput in comparison to the possible throughput without handover means that TCP does not utilize the available bandwidth of the underlying network.

5.4.2. Scalability

Scalability is of particular importance for mobile networks since these systems are required to support a high number of mobiles hosts. On the one hand, the use of multicast for mobility scheme demands for a scalable multicast routing protocol. Unfortunately, the ASM service model of IP is designed for a high number of hosts per group. Each multicast group generates a certain amount of multicast states in routers. The routing table size is a concern since multicast routing does not support aggregated routing as unicast routing and large routing tables imply a high signaling overhead for exchanging the routing state among the routers. In a multicast-based mobility scheme where a unique multicast group is used per mobile host and a multicast group has only a few members, the scalability with the number of multicast groups is an important evaluation criterion. On the other hand, signaling overhead on the wireless link is associated with higher costs than on links of the wire-line backbone. While the exchange of multicast routing state among routers pertains to the backbone, the signaling between the mobile host and the access points can consume large portions of the wireless link bandwidth and limit the scalability.

5.5. Summary

For the quantitative performance evaluation of the mobility schemes a combination of measurements, simulation, and analytical evaluation is selected. These evaluation techniques are used complementarily instead of exclusively and are a consequence of the complexity of the investigated system. Measurements are applied to investigate mobility-related performance metrics, such as handover latency and packet loss. These measurements are conducted with a physical model of the real system. Analytical modeling is applied to evaluate scalability effects, such as the calculation of the aggregated signaling load in a wireless network using a more simplified network model. Analytical modeling is also applied to verify the results gained by measurements.

The evaluation process based on measurements basically consists of four parts: the particular mobility management scheme, the network model, workload generation, monitoring and data collection, and finally statistical evaluation. The mobility scheme and the network model form the system model. The workload inputs that system model and results in a certain system output that is monitored and evaluated.

Finally, handover performance in terms of handover latency, packet loss and duplication for UDP traffic, and TCP throughput are defined as evaluation criteria.

6. Protocol Design for the Selected Case Studies

In Chapt. 4 the developed framework was used to derive four case studies for multicast-based mobility support to be investigated within the thesis. In order to realize the mobility support functions that augment the multicast, an information exchange between the components of the system is necessary. The interactions are governed by protocols. The design of these protocols is presented in this chapter. The protocol design is the basis for the software platform and the prototype implementation that will be described in Chapt. 7.

The case studies have been determined by choosing certain protocol options. Some of the protocol options are different in all case studies. An example of an unequal protocol option is the multicast type. As a consequence of the different protocol options the protocol design for the augmenting mobility functions for each case study is different as well. However, the protocol design can be grouped into two classes: The first class is comprised of the case studies MB-ASM, MB-SSM, and MB-CMAP. These case studies have many similarities and therefore a common treatment is justified. In fact, the software platform – that will be described in Chapt. 7 – has been used for experimentation with the three case studies. For the fourth case study MIP-SGM the protocol design is fundamentally different from the other case studies since MIP-SGM is not based on multicast as the basic mobility mechanisms. MIP-SGM relies on *indirect addressing and address translation* (see Sect. 2.5). The protocol design for augmenting the basic and hierarchical Mobile IP is therefore treated separately. This fundamentally different protocol design is the reason that the developed prototype could not be used for the case study MIP-SGM.

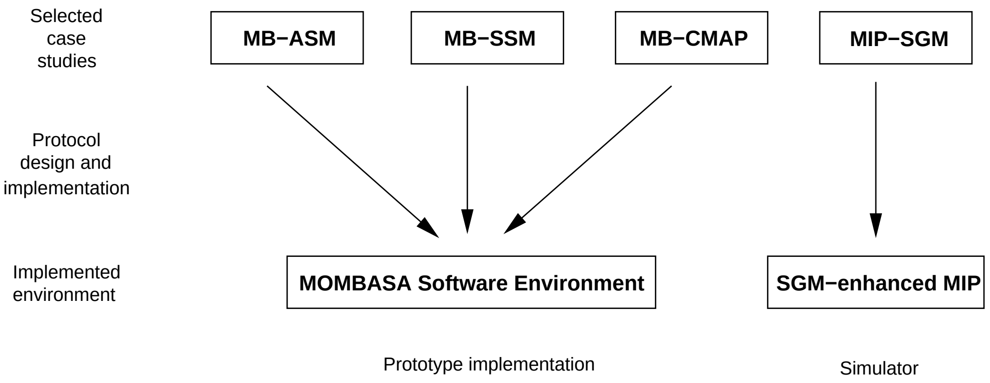


Figure 6.1.: Overview of the protocol design for the case studies

In the following the protocol design and prototype implementation for the first class of case studies MB-ASM, MB-SSM, and MB-CMAP will be termed *MOMBASA Software Environment*

(MOMBASA SE). It is common to these case studies that they require multicast protocols for group management and routing. Also, there are other common protocol options bearing resemblance that justify a unified treatment. As an example, the multicast endpoint is located in the access point. As a consequence, the multicast protocol for group management is not employed on the wireless link between the access point and the mobile host. New protocols are required for basic mobility functions such as registration of mobile hosts and others pertaining to the mobile host. Clearly, such functions can be realized by protocols common to all three case studies.

In general, the protocols manage the communication between the particular components of the system, namely between the mobile host and the access point, among the access points themselves, as well as between the access point and the gateway. On the one hand, for most of the protocol operations the multicast scheme can be regarded as a certain service offered by the access network. Continuing the above example – the registration of the mobile host with an access point – the access point subscribes to the multicast group that corresponds to the mobile host. The subscription to the multicast group is common to all variants in MOMBASA SE, and for the protocol design it is sufficient to regard this as a generic multicast operation, although the detailed multicast operation for subscribing to the multicast group is unique to the multicast type. On the other hand, certain features of the multicast types result in different protocol operations. For example, the function to pre-register a mobile host with an access point in advance of a handover can be realized either by an inter-access point protocol or by third party signaling. If the multicast type supports third party signaling, there are no protocol operations required among the access points.

Using the options for protocol design and mobility functions for the case studies as selected in Sect. 4.6 results in a great number of possible combinations. Constructing a solution that supports all combinations seems possible, but might become impractically. Therefore, the number of possible options for handover are limited. Three main handover policies are defined with respect to the mobility functions for handover detection, rerouting, and buffering (Tab. 6.1). The selected combinations have been chosen to meet application requirements for handover with a small service interruption (soft handover), with small packet loss (predictive handover), and with no specific requirements, but with a small protocol overhead (hard handover). In Tab. 6.2[1] is listed which handover policies are supported by the case studies.

Handover policies	Hard	Soft	Predictive
Handover detection	Lazy	Eager	Lazy
Rerouting	Break-Make	Make-break	Make-break
Buffering and forwarding	No	No	Yes

Table 6.1.: Definition of basic handover policies

The chapter is structured into two main sections. The first section presents the protocol design for MOMBASA SE, the second section describes the protocol design for the fourth case study MIP-SGM. The first section about MOMBASA SE includes the following issues. At first, a system overview is given and a generic multicast service defined. Then, the addressing and address translation is explained, the meaning of dedicated multicast groups described, and the basic data transport illustrated. Then, the protocol operations are given, first in a generic manner and then including some details of the multicast scheme.

[1] The case study MIP-SGM supports hard handover. This case is equivalent with the handover in basic and hierarchical Mobile IP

Handover policy	Hard	Soft	Predictive
MB-ASM	No	Yes	Yes
MB-SSM	No	Yes	Yes
MB-CMAP	Yes	Yes	Yes
MIP-SGM	Yes	Yes	No

Table 6.2.: Basic handover policies used in the case studies

6.1. Protocol Design for the Case Studies MB-ASM, MB-SSM, and MB-CMAP

Principally, a protocol can be described by [83]

1. its offered service,
2. the assumptions about the environment,
3. the vocabulary of the messages,
4. the encoding of each message, and
5. the procedure rules.

In this section the offered services, assumptions about the environment and procedure rules (issue 1,2, and 5) are presented. For the detailed vocabulary of messages and their encoding (issue 3 and 4), it is referred to the specification of MOMBASA SE. This specification is based on Specification and Description Language (SDL) [50], a general-purpose specification language for communication systems. The system is modeled as communicating processes of the components and their environment. Each process is regarded as an Extended Finite State Machine (EFSM).

The specification is summarized in [59]. The specification of the particular multicast protocol can be found in [55] (IGMPv2), [25] (IGMPv3), [54] PIM-SM and PIM-SSM, [40] (CMAP), and [45] (CMNP).

6.1.1. System Overview

The scope for the MOMBASA SE protocol design is micro mobility. Global mobility support is assumed to be handled by an appropriate protocol. As described in Chapt. 2, Mobile IP can be regarded as the classical solution for global mobility support in IP networks, however, the expected convergence of IP-based networks and classical telecommunication networks has resulted in alternative application-layer approaches, such as ICEBERG [161] and MPA [7, 105, 140]. Instead of specifying a particular protocol for global mobility support protocol, for the protocol design of MOMBASA SE it is only assumed that the protocol for global mobility offers a service for location and mobility management in the global Internet. For example, this service can be realized by *personal proxies* as in the MPA approach. This service includes not necessarily the support of handover for the case that a mobile host moves from one access network to another. For the design of the protocols a system with the following instances is assumed (see Fig. 6.2):

Gateway (GW). The gateway is a network node that connects the access network to the global Internet. It receives packets from the Internet and forwards them towards the mobile host along the multicast distribution tree. In general an access network may have multiple gateways. The gateway translates the in-bound packets to an appropriate format for forwarding them on to the multicast distribution tree, by network address translation from IP unicast to the IP multicast packets[2] or by segmentation of packets into cells (MB-CMAP). The gateway hosts also the so-called **Gateway Proxy (GWP)** used for paging. In case of bi-directional multicast (e.g. CMAP/CMNP in the case study MB-CMAP), the gateway proxy also manages multicast groups.

Multicast Node (MCN). The Multicast Node (MCN)s form the backbone of the access network. They have no special mobility-related functionality. They are either standard IP unicast and multicast routers (MB-ASM, MB-SSM) or multicast-capable cell switches (MB-CMAP).

Access Point (AP). The access point is a network node connecting the last hop to the access network backbone. In relation to the multicast node an access point acts as a multicast receiver (or member of multicast groups). In the case of MB-ASM and MB-SSM multicast packets received from the access network are translated to unicast and sent to the mobile host. In the case of MB-CMAP the received cells are reassembled to IP packets and forwarded to the mobile host. The access point hosts the so-called **Mobility Enabling Proxy (MEP)** that is responsible for mobility-related tasks such as last hop signaling, signaling to neighboring access points and to the Gateway Proxy, and management of the mobility-related multicast groups as a surrogate member.

Mobile Host (MH). The mobile host is an IP host with possibly multiple interfaces of different wireless technologies moving within the area covered by the access network. The mobile host executes a *Mobile Agent* that is responsible for the last hop signaling and detection of inactive (i.e. idle) state.

6.1.2. Services Offered by the Protocols

The protocols offer the following services to a mobile host:

- Initial registration, re-registration and de-registration of a mobile host with an access point,
- Pre-registration of a mobile host with neighboring access points, either by the current access point (MB-ASM and MB-SSM) or by the multicast node (MB-CMAP),
- Detection, triggering and signaling of handover for active mobile hosts between access points belonging to the same access network,
- Support of different handover types: hard, soft, and predictive,
- Location update for inactive mobile hosts,
- Paging to determine the current access point of an inactive mobile host; the paging itself is based on multicast,
- Buffering of packets during an ongoing paging process and forwarding of the packets after a successful paging process,

[2] Network Address Translation (NAT) for MB-ASM, and IP-in-IP encapsulation and tunneling for MB-SSM.

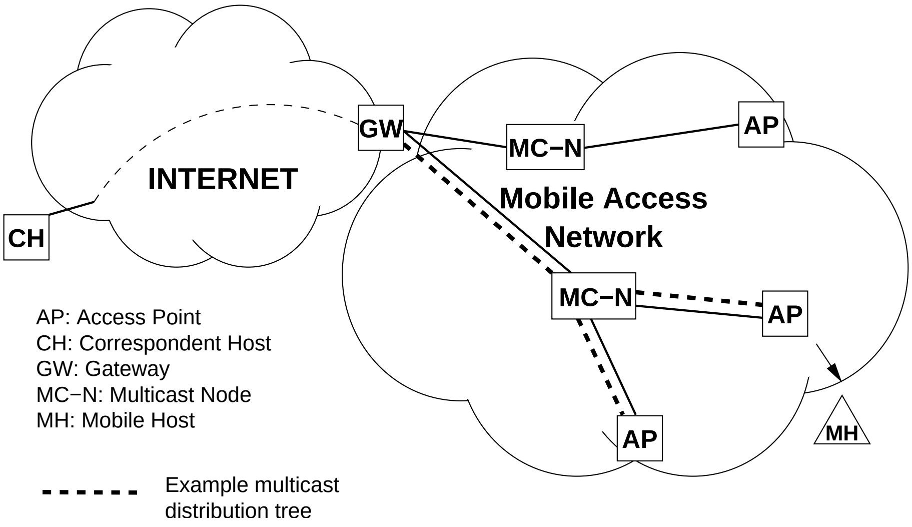


Figure 6.2.: System architecture

- Buffering of packets for a pre-registered mobile host and forwarding of the buffered packets when the mobile host registers directly.

6.1.3. Generic Multicast Services

It is assumed that the access network offers the following multicast service:

- Identification and addressing of a multicast group and multicast receivers,
- Creation of a multicast group,
- Subscription to a multicast group,
- Creation, modification, and release of a multicast distribution tree,
- Data transport along the multicast distribution tree,
- Un-subscription of a host from a multicast group,
- Destruction of a multicast group.

The following Tab. 6.3 illustrates how the generic service can be mapped to the multicast type of the particular case study.[3]

6.1.4. Addressing and Address Translation

Each mobile host is uniquely identified by a unicast IP address that does not change as long as the mobile host remains in the access network. The unicast address belongs to the address realm of the access network. The IP address is assigned to the mobile host when it enters the access network for

[3] In Tab. 6.3 MC stands for multicast, and UC for unicast.

Case study	**MB-ASM**	**MB-SSM**	**MB-CMAP**
MC management protocol	IGMPv2	IGMPv3	CMAP
MC routing protocol	PIM-SM	PIM-SSM	CMNP
Group identity	Receiver group	Receiver group (Multicast channel)	Group of senders and receivers (Multipoint call)
Addressing	Multicast IP address	Channel ID Multicast IP address & UC IP address of source	CMAP Call ID
Group creation	IGMPv2 Join (Implicit)	IGMPv3 Join (Implicit)	CMAP Open_Call
Subscription	IGMPv2 Join	IGMPv3 Join	CMAP Add_Endpoint
Data transport	Packet forwarding	Packet forwarding	Cell switching
Un-subscription	IGMPv2 Leave	IGMPv3 Leave	CMAP Drop_Endpoint
Group destruction	IGMPv2 Leave (Implicit)	IGMPv3 Leave (Implicit)	CMAP Close_Call
Creation, modification and release of the multicast distribution tree	PIM-SM Join and Leave	PIM-SSM Subscribe and Un-subscribe	CMNP Net_Create_CG Net_Join_CG, Net_Mod_CG, Net_Destroy_CG, etc.

Table 6.3.: Mapping of the generic multicast service to specific multicast operations in the case studies of MOMBASA SE

the first time and this assignment is deallocated when the mobile host leaves the access network. The unicast IP address can be assigned by well-known protocols such as DHCP [49].

To the unicast IP address a multicast address is associated in a one-to-one manner. The multicast address is internally used only within the access network. The type of the multicast address depends on the multicast scheme (see Tab. 6.3): a class-D IP multicast address in the case study MB-ASM, a multicast channel (a tuple of unicast IP address of the multicast tree source and a class-D IP multicast address) in MB-SSM, or a call identifier (a tuple of the identifier of the root node and an unique identifier of the tree termed local identifier) in MB-CMAP.

In order to transport IP packets by means of multicast in the access network, the IP packets must be modified to be carried by the multicast distribution tree. For IP multicast this means an address translation from unicast to multicast addresses, either by NAT or by IP-IP encapsulation and tunneling [53, 128, 130]. The address translation from unicast to multicast addresses is performed in the gateway, the access points reverse the process by executing the address translation from multicast back to unicast. While for the case study MB-ASM, both NAT and IP-IP encapsulation/tunneling is possible, for the case study MB-SSM encapsulation and tunneling is even necessary. This is due to the fact that with single-source multicast SSM the source address is also part of the multicast channel identifier. A packet sent along the multicast tree must carry the IP address of the source of the tree. If NAT translation was be used, then the source address of the packet would have to be translated as well. This in turn would mean that the information about source of the packet, i.e. the address of the correspondent host, would be lost. In order to preserve this information, encapsulation and tunneling instead of NAT must be applied.

In the case study MB-CMAP the underlying transport technology is cell switching. Therefore, IP packets entering the access network are segmented into cells carrying their own addressing information in the gateway and reassembled to IP packets in the access point. For the reverse direction from the access point to the gateway packets are segmented into cells in the access point and reassembled in the gateway.

6.1.5. Dedicated Multicast Groups

The following dedicated multicast groups exist:

Mobile Host Groups Each mobile host has an associated multicast group. In the case of MB-ASM (and similar in MB-SSM) the unicast IP addresses and corresponding multicast addresses of mobile hosts form continuous blocks of equal size that can be mapped easily into each other by bit-mapping. In MB-CMAP, the unicast IP address is mapped one-to-one to the CMAP call identifier of the multicast group.

MEP Groups Neighboring access points with their MEPs form a MEP group that is represented by a multicast group. When a mobile host registers with a MEP and requests a predictive handover, then this mobile host will be pre-registered with all the other MEPs belonging to the MEP group. The pre-registration is executed indirectly either via the other MEP or via the multicast node. The latter scheme for indirect registration requires *third-party signaling* from the multicast scheme.

Paging Areas When a mobile host is inactive, it registers less frequently. In this case the network is provided with an uncertain location information. Hence, the mobile host must be located in order to establish a multicast distribution tree that includes the current access point of the mobile host and to trigger a mobile host activity and enabling it to receive data. In MOMBASA SE this is done by sending a paging request to a group of MEPs where the mobile host is suspected to be. Such a group of MEPs is called paging area and is also represented by a multicast group. Usually a paging area is formed by neighboring MEPs. In comparison to a MEP group, the size of a multicast group for a paging area is larger, typically of geographical dimension.

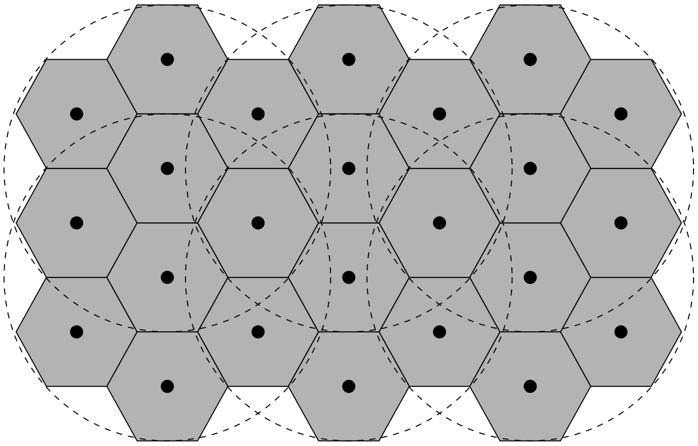


Figure 6.3.: Overlapping paging areas

6.1.6. Data Transport

For the transport of packets the direction of the traffic flow must be distinguished. Downstream traffic is sent from a correspondent host via the gateway along the multicast distribution tree to the mobile host. If the multicast supports bidirectional transport of data (as CMAP in the case study MB-CMAP), then the uplink traffic will be transported by a multicast distribution tree as well. Otherwise (as in the case studies MB-ASM and MB-SSM that support unidirectional multicast trees from the gateway to the access points) upstream traffic is transported by unicast routing.

Downstream traffic from a correspondent host to the mobile host is transported as follows:

1. The correspondent host sends the data packets to the mobile host's unicast IP address.

2. Since the mobile host's unicast IP address lies within the address space of the access network, the packets reach the gateway by standard Internet routing mechanisms.

3. The gateway performs address translation (NAT or encapsulation) and segmentation, respectively, and forwards the data (packet or cells) on the corresponding multicast distribution tree if it exists. If the multicast distribution tree (and the multicast group) does not exist but a corresponding entry is found in the gateway proxy's paging table, paging will be started in order to locate the mobile host and the packets will be buffered in the gateway proxy.

4. The data packets are forwarded to the MEPs that have subscribed to the mobile host's multicast group within the access network.

5. a) The MEP at which the mobile host is directly registered executes the reverse address translation to the mobile host's unicast IP address (or reassembles the cells to IP packets) and forwards them to the link from which the mobile host has registered.

b) The passive MEPs belonging to the MEP group buffer the packets in a ring buffer. If the mobile host performs handover to a passive MEP the buffered packets will be forwarded to it to compensate for the packets lost during the handover latency.

6. The packets arrive at the mobile host as normal unicast IP packets.

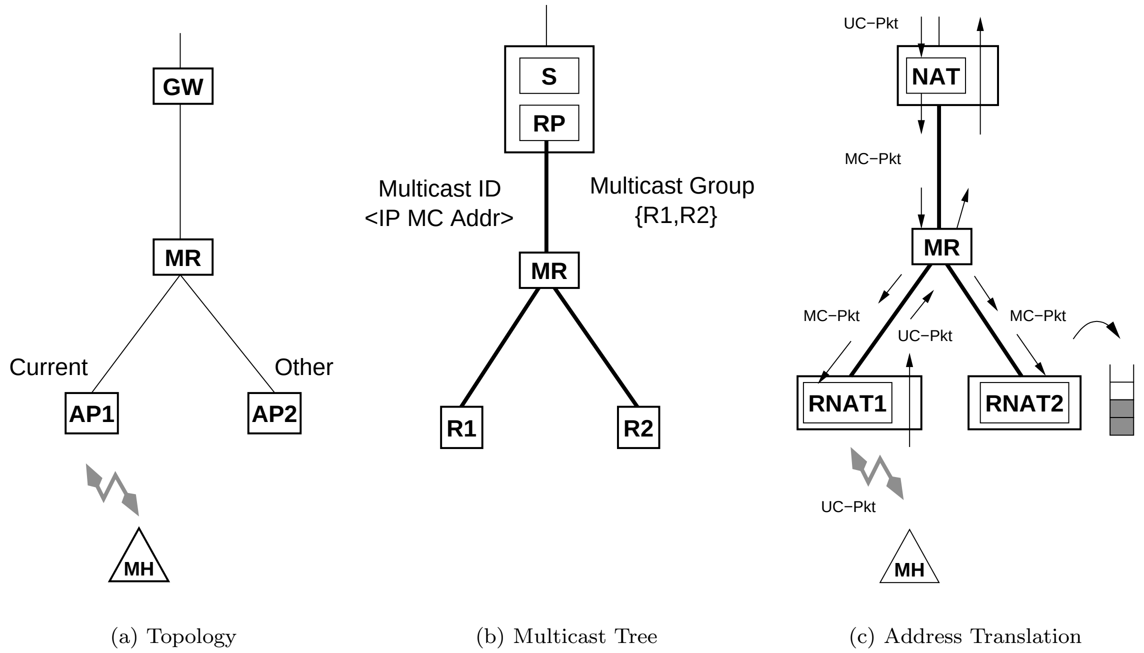
Upstream traffic originating from the mobile host and using unidirectional multicast distribution trees (as in the case studies MB-ASM and MB-SSM) is sent and routed as normal unicast packets.

With bi-directional multicast trees (as in the case study MB-CMAP), upstream traffic originating from the mobile host is transported as follows:

1. The mobile host sends the data packets to the MEP the mobile host is registered with.
2. The MEP segments the packets into cells and forwards them on the multicast distribution tree that corresponds to the mobile host.
3. The gateway receives the cells, reassembles them into IP packets and forwards the packets to the correspondent host using standard unicast routing mechanisms.
4. Due to the bidirectional multicast tree, the other MEPs belonging to the MEP group receive the cells as well. However, these cells are discarded.
5. The packets arrive at the correspondent host as usual unicast packets.

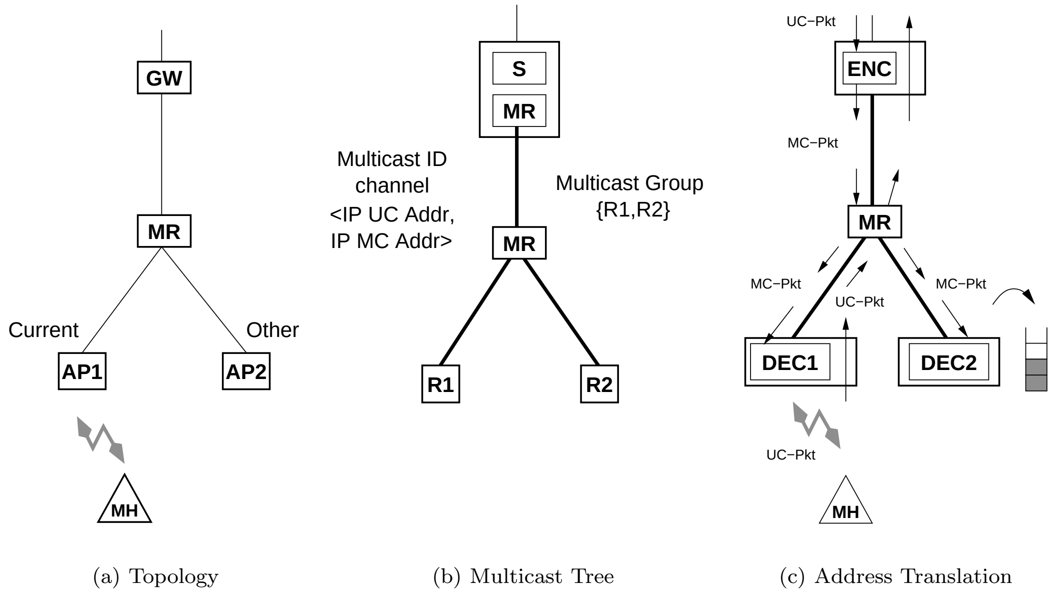
The data transport is illustrated in the following figures[4]: Fig. 6.4 for the case study MB-ASM, Fig. 6.5 for the case study MB-SSM, and Fig. 6.6 for the case study MB-CMAP. Each figure consists of three sub-figures. The first sub-figure (a) draws the exemplary topology of the access network. The second sub-figure (b) shows a possible multicast tree. The third sub-figure explains the address translation for each case study. In all figures normal edges represent physical interconnections and bold edges are branches of a multicast tree.

[4] The following abbreviations are used in the figures: AP – Access Point, DEC – Decapsulation, ENC – Encapsulation, EP – Endpoint, GW – Gateway, MH – Mobile Host, MR – Multicast Router, NAT – Network Address Translation, R – Receiver, RNAT –Reverse Network Address Translation, RP – Rendezvous Point, S – Sender, SAR – Segmentation and reassembling, SW – Switch.



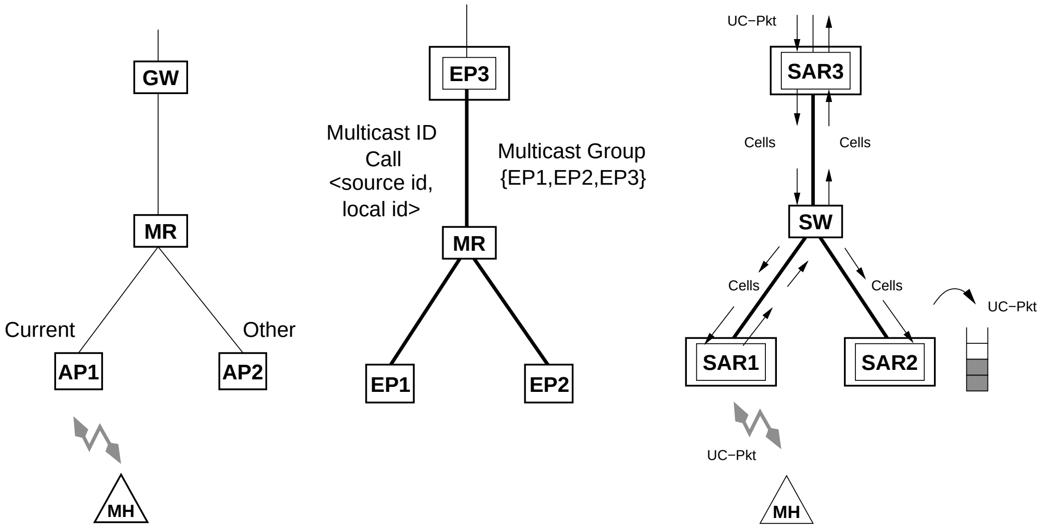
(a) Topology (b) Multicast Tree (c) Address Translation

Figure 6.4.: Exemplary data transport in MB-ASM



(a) Topology (b) Multicast Tree (c) Address Translation

Figure 6.5.: Exemplary data transport in MB-SSM



(a) Topology (b) Multicast Tree (c) Address Translation

Figure 6.6.: Exemplary data transport in MB-CMAP

6.1.7. Protocol Operations

In this section the basic protocol operations are described and depicted by time-line diagrams. The diagrams with multiple access points assume that the access points have the same designated multicast node in order to keep the diagrams as simple as possible.

Initial Registration

The mobile host initially registers with the MEP when it enters the access network for the first time after it has acquired a unicast IP address. The current MEP can pre-register the mobile host with another MEP belonging to its MEP group. The time-line of the initial registration using generic multicast operations is shown in Fig. 6.7. In Fig. A.1(a) and A.1(b) in Appendix A the specific multicast operations are detailed. Initial registration happens as follows:

1. a) The access point advertises its availability frequently (or as a response to a solicitation) on all downstream interfaces.

   b) If third-party signaling is not supported by the multicast service an *Inter-MEP Advertisement* is sent to the local MEP group in a regular time interval containing the addresses of the directly registered mobiles.

2. The mobile host sends a *MH Registration Request* with a flag indicating its active state to the MEP.

3. The MEP inserts the mobile host into its registration table, subscribes to the corresponding multicast group, and sends a *MH Registration Reply* to the mobile host.

   - Pre-registration via MEP: The new mobile host is included in the next *Inter-MEP Advertisement.* Then the other MEPs in the MEP group also subscribe to the mobile host's multicast group on reception of this advertisement.
   - Pre-registration via MC-N: The active MEP subscribes to the multicast group on behalf of the other MEPs belonging to the MEP group.

Handover

A handover is executed when the mobile host decides to change the access point. Three types of handover are distinguished: hard, soft, and predictive (see Sect. 2.1). The time-line diagrams for all handover types are shown in Fig. 6.9 – 6.11. The detailed multicast protocol operations can be found in Fig. A.2 – Fig. A.5 in Appendix A. In the following, only the predictive handover with generic multicast operations is explained and a handover scenario with four access points (see Fig. 6.8) is used. In this scenario two MEP groups exist that are comprised of the respective neighboring access points. The first MEP group consists of the old access and the new access point and another access point (*Other AP2*). The second MEP group contains *Other AP1* instead of *Other AP2.* Hence, in order to update the MEP group, a single subscribe and un-subscribe operation is needed.

The other handover cases (hard, soft) are self-explanatory by means of the figures.

For a predictive handover the following steps are executed:

1. The mobile host detects the availability of new access points when it receives their *MEP Advertisements.*

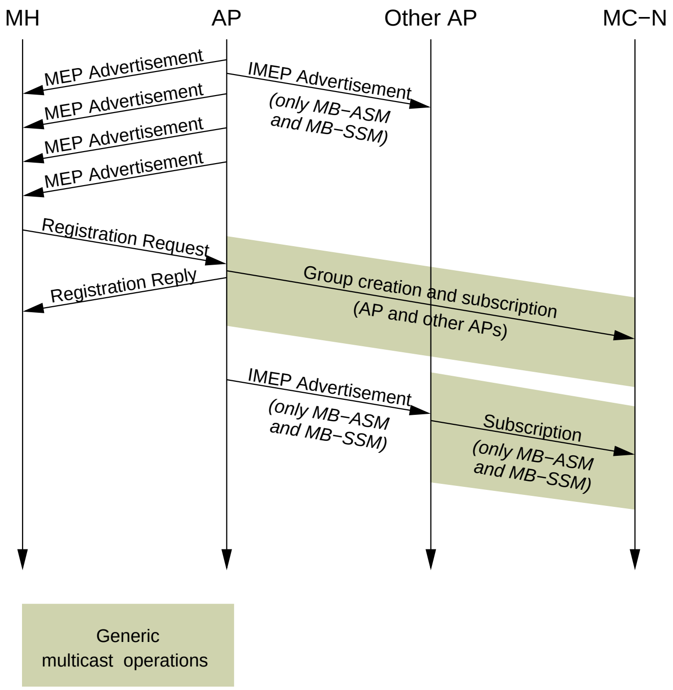


Figure 6.7.: Time-line: Registration with generic multicast operations

2. When a handover is triggered by expiration of a MEP advertisement lifetime (or by other mechanisms, such as link-layer trigger indicating that the signal strength is below a threshold or by determining a higher priority of the new MEP advertisement) the mobile host sends a *MH Registration Request* to the MEP.

3. If the mobile host is already pre-registered, the registration table will be updated and the buffered packets will be flushed to the mobile host. Otherwise the MEP will insert the mobile host into its registration table and subscribe to the corresponding multicast group. In any case it sends a *MH Registration Reply* to the mobile host.

4. The mobile host may send a de-registration (registration request with lifetime zero) to the old MEP.

5. When the old MEP receives the de-registration or when the registration in the MEP expires, the MEP un-subscribes from the mobile host's multicast group. The MEP group is updated:

   - Pre-registration via MEP: The mobile host will not be included in its next *Inter-MEP Advertisement* and the MEPs in the old MEP's group that are not in the new MEP's group will un-subscribe from the mobile host's multicast group as well.[5]
   - Pre-registration via MC-N: The new MEP inspects the existing MEP group and adds and drops MEPs to/from the MEP group accordingly.

[5] Direct registrations take priority over indirect registrations. However the indirect ones are not discarded but noted in the registration table. If the direct registration becomes invalid (either because it expires or the mobile host is de-registered) the indirect registration will take over and the MEP will become passive.

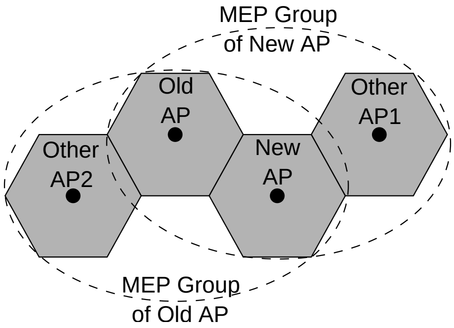


Figure 6.8.: Scenario for predictive handover

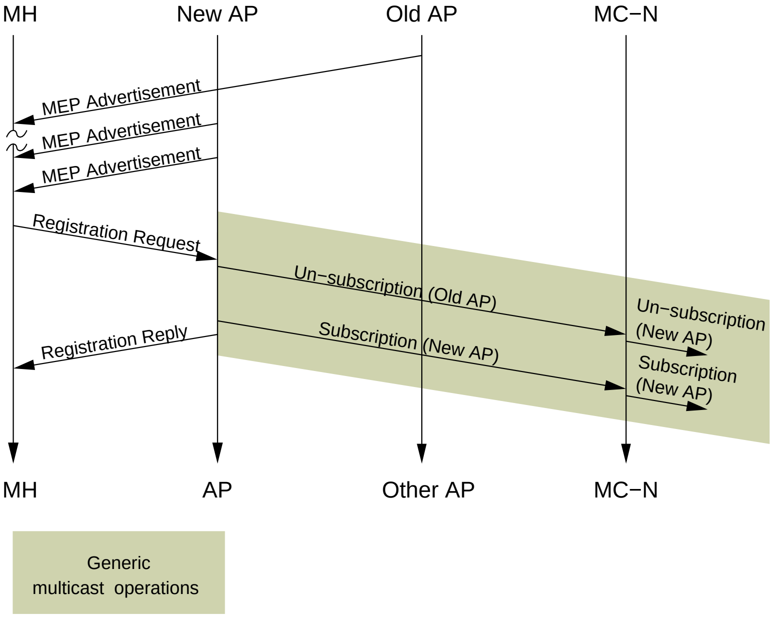
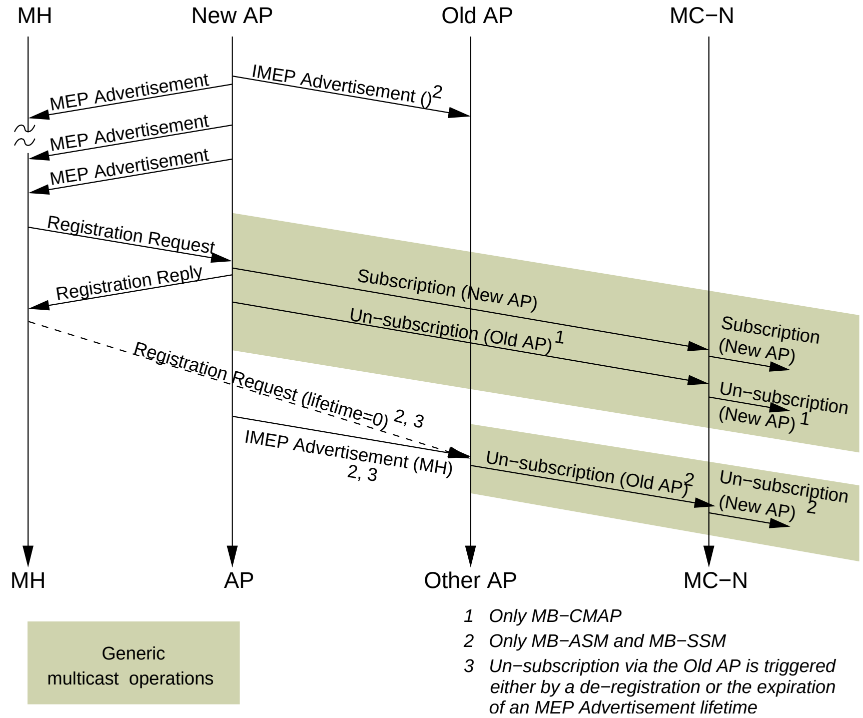


Figure 6.9.: Time-line: Hard handover with generic multicast operations


MH
New AP
Old AP
MC−N
IMEP Advertisement ()2
MEP Advertisement
MEP Advertisement
MEP Advertisement
Registration Request
Registration Reply
Subscription (New AP)
Un−subscription (Old AP) 1
Subscription (New AP)
Un−subscription (New AP) 1
Registration Request (lifetime=0) 2, 3
IMEP Advertisement (MH) 2, 3
Un−subscription (Old AP) 2
Un−subscription (New AP) 2
MH
AP
Other AP
MC−N
Generic multicast operations

1 Only MB−CMAP

2 Only MB−ASM and MB−SSM

3 Un−subscription via the Old AP is triggered either by a de−registration or the expiration of an MEP Advertisement lifetime

Figure 6.10.: Time-line: Soft handover with generic multicast operations

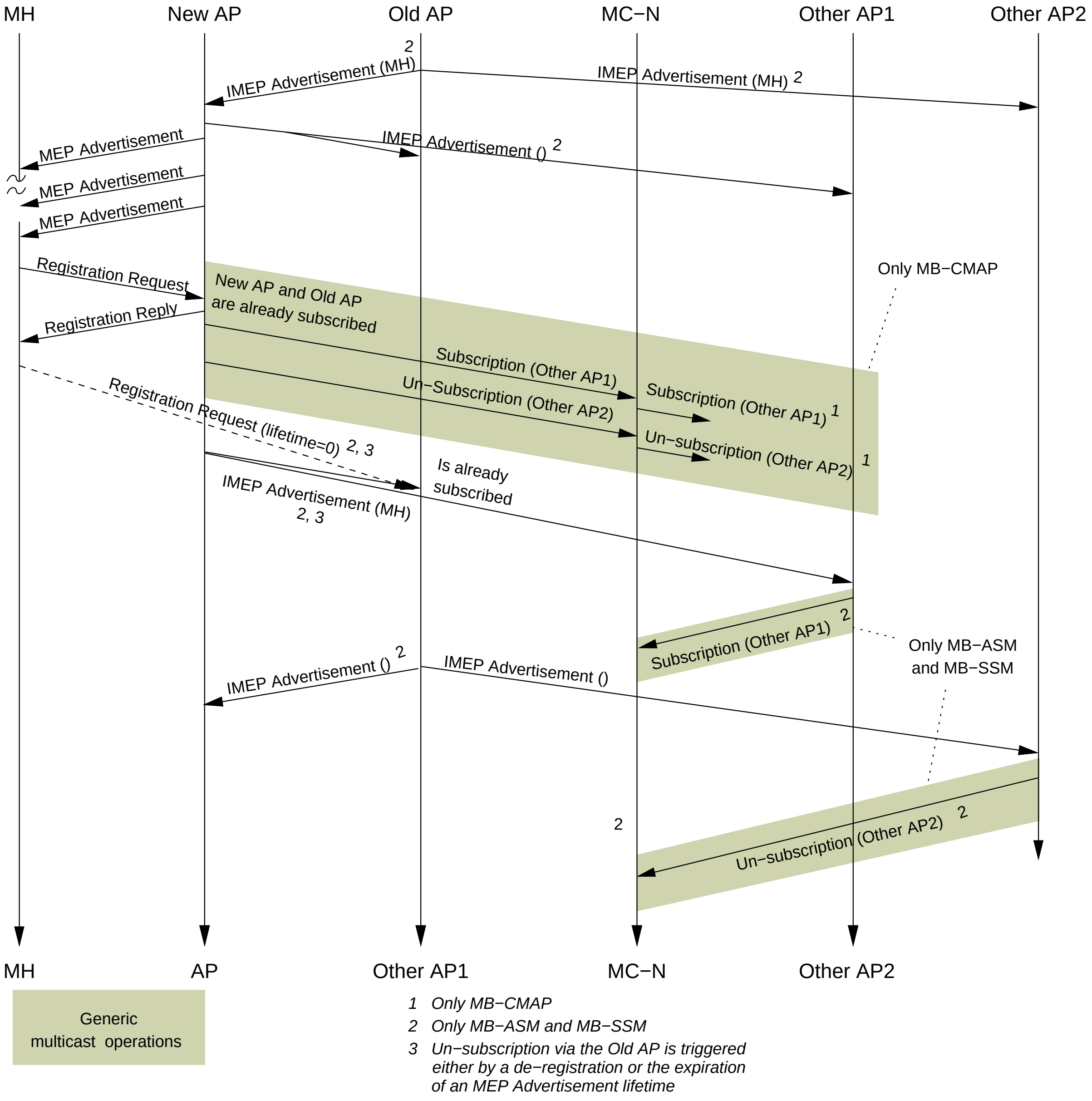


Figure 6.11.: Time-line: Predictive handover with generic multicast operations

Switching Between Active and Inactive Mode

When for some time the mobile host has neither received nor sent data traffic it switches to the inactive mode. In this mode the mobile host re-registers less frequently and the corresponding multicast group does not exist. The time-line diagram in Fig. 6.12 shows the switch from active to inactive mode and back to active mode with generic multicast operations. The operations specific to a multicast scheme are drawn in Fig. A.6(a) and A.6(b).

1. The mobile host sends a *MH Registration Request* indicating its inactive state to a selected MEP.
2. If the mobile host has been registered at this MEP the registration entry will be removed and the MEP will un-subscribe from the mobile host's multicast group.
3. The MEP sends a *Paging Update* with the paging area associated to the current location to the Gateway Proxy.
4. The Gateway Proxy enters the mobile host and its location (paging area) into its paging table.
5. If possible the mobile host should send a de-registration to the old MEP (if it is different from the new one). Otherwise the multicast group will remain intact until the registration in the old MEP will expire.

The mobile host wakes up (switches from inactive to active mode) either when it attempts to send data or when it receives a *Paging Request* (see also next section). The sequence of messages is also shown in Fig. 6.12.

1. The mobile host sends a *MH Registration Request* indicating its active state to a MEP and thereby informs the MEP that it is in the process of wake-up.
2. The MEP inserts the mobile host into its registration table, subscribes to the corresponding multicast group and sends a *MH Registration Reply* to the mobile host. Since the wake-up flag is set, a *Paging Update* with lifetime zero is sent to the Gateway Proxy.
3. The Gateway Proxy removes the paging table entry on reception of the *Paging Update*.

Paging

When the Gateway Proxy receives a data packet for an inactive mobile host (i.e. a host for which an entry in the paging table exists) it starts paging (see Fig. 6.13 for the generic multicast operations and Fig. A.7(a) and A.7(b) for multicast-specific operations):

1. The Gateway Proxy starts buffering of the packets for this mobile host and sends a *Paging Request* to the last reported paging area.
2. The MEPs in the paging area (i.e. members of the paging area multicast group) receive the *Paging Request* and forward it onto the downstream interfaces.
3. The mobile host receives the *Paging Request* (possibly multiple times) and performs the wake-up procedure described in the previous section.
4. After having received the *Paging Update* with lifetime zero the Gateway Proxy waits for the related multicast group to become existent. In this case the buffered packets are sent to the multicast group and paging is finished.

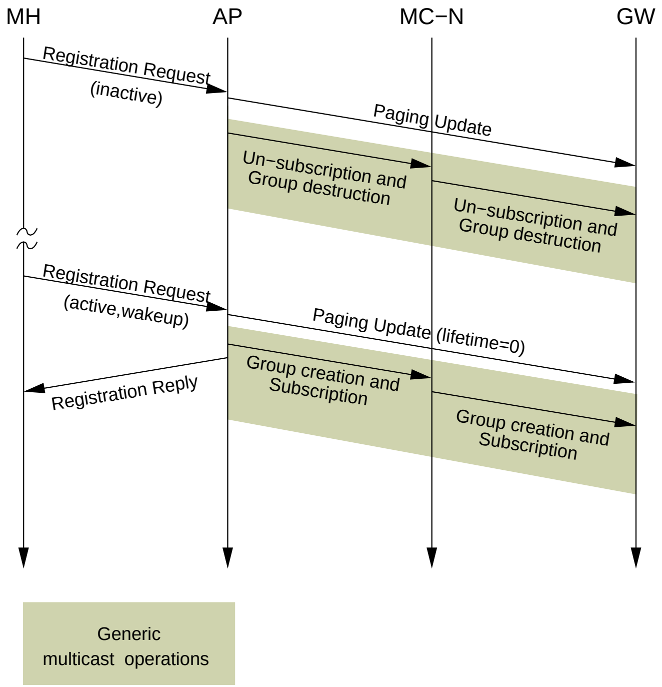


Figure 6.12.: Time-line: Switching to inactive mode and back to active mode with generic multicast operations

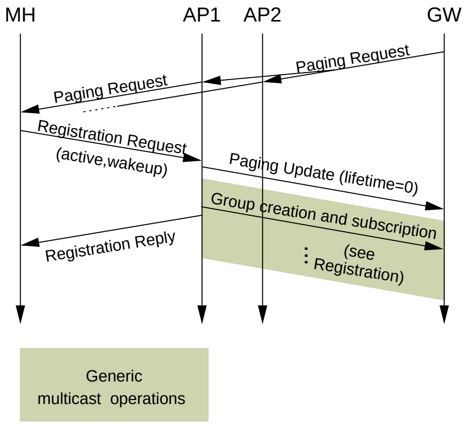


Figure 6.13.: Time-line: Paging with generic multicast operations

6.2. Protocol Design for the Case Study MIP-SGM

This section describes the protocol design for the case study MIP-SGM. The mobility mechanism of this case study is based on Mobile IP and hierarchical Mobile IP, respectively. Since the protocols are described in [70, 129] and have been briefly explained in Sect. 2.5 and 2.7, only the extensions of Mobile IP and hierarchical Mobile IP are presented.

6.2.1. Soft Handover in SGM-Enhanced Basic Mobile IP

In the basic Mobile IP the home agent has only a single binding between the mobile host's home address and care-of-address. When a mobile host sends a binding update, the old binding is replaced by the new one. The principal idea of the SGM extension is to enable the home agent to send data packets to multiple foreign agents. For soft handover the data packets are tunneled to the old and to the new foreign agent. In order to set up multiple tunnels between the home agent and the foreign agents, the home agent must be able to maintain multiple bindings simultaneously (also called simultaneous binding).

In Fig. 6.14 a soft handover with Mobile IP is shown.[6] The following steps are executed:

1. The mobile host detects the availability of new access points when it receives their *Agent Advertisement*.

2. When a handover is triggered by expiration of an agent advertisement lifetime, the mobile sends a *Registration Request* that contains the new CoA that has been advertised by the new foreign agent to the new foreign agent. In the request a flag is set that forces a simultaneous binding.

3. The foreign agent checks the *registration request* and relays the request to the home agent.

4. When the home agent receives the *Registration Request*, it updates its registration table. Since the request has indicted a simultaneous binding, the binding with the old care-of-address is not deleted. The home agent sends a *Registration Reply* back to the mobile host.

5. New data packets arriving at the home agent will be encapsulated into SGM packets, i.e. the outer packet header contains two destination addresses, namely the old and the new CoA.

6. The foreign agent intercepts the *Registration Reply*, updates its registration table, and relays the reply to the mobile host.

7. In order to complete the handover process, the mobile host sends a *Registration Request* with the old CoA and with lifetime zero to the foreign agent.

8. The foreign agent relays the *Registration Request* to the home agent.

9. The home agent removes the binding with the old CoA from its registration table and replies to the request.

10. The foreign agent relays the reply to the mobile host. The mobile host receives the reply.

11. New data packets arriving at the home agent will not be encapsulated into SGM packets any more.

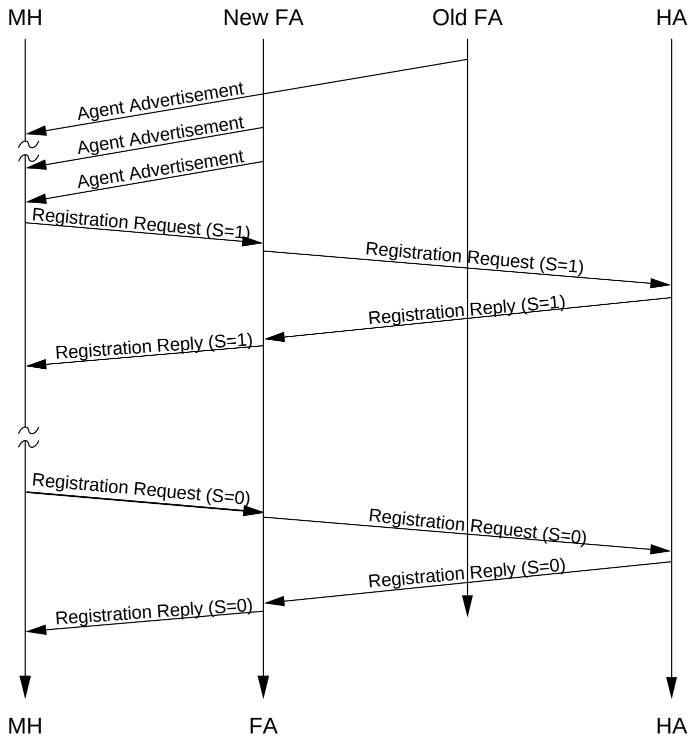


Figure 6.14.: Time-line: Soft handover in MIP-SGM

For generating a simultaneous binding the Mobile IP standard offers a flag termed *S-bit*. This flag forces the home agent to retain the binding to the old CoA. However, MIP-SGM does not depend on this option. As stated by [75], without the S-bit simultaneous bindings can still be deployed, but the home agent's will be responsible to set them up. If the previous binding to the old CoA is kept by default, the mobile host can explicitly remove this binding by a de-registration request with lifetime zero.

6.2.2. Soft Handover in SGM-Enhanced Hierarchical Mobile IP

In SGM-enhanced hierarchical Mobile IP the switching foreign agent is enabled to send SGM packets to multiple lowest foreign agents. The procedure for soft handover with hierarchical Mobile IP enhanced by SGM is the same as with basic Mobile IP enhanced by SGM, except that the simultaneous binding exists in the switching foreign agent instead of the home agent. Registration requests are not send to the home agent, but to the switching foreign agent.

[6] For all Mobile IP considerations, a *foreign agent care-of-address* (not *co-located care-of-address*) is assumed.

6.3. Summary

In this section the protocol design for the selected case studies was presented. The design comprises the protocols to augment the particular multicast by mobility support functions. The similarity of the multicast schemes in case studies MB-ASM, MB-SSM, and MB-CMAP has facilitated a unified protocol design. For the case study MIP-SGM the extensions of the basic and hierarchical Mobile IP have been described. The extensions utilize simultaneous bindings between the home address and the old/new care-of-address.

7. Software Platform

For the case studies MB-ASM, MB-SSM, and MB-CMAP a software platform has been implemented termed *MOMBASA Software Environment (MOMBASA SE).* As will be explained in this chapter, the software platform is not limited to the case studies investigated in this thesis and can rather be regarded as an experimental platform to investigate multicast-based mobility support in IP networks targeted for research.

The implementation is based on the protocol design presented in Sect. 6.1 and the specification described in [59]. The implementation is open-source software under the GNU General Public License (GPL) [69] and publically available at
`http://www-tkn.ee.tu-berlin.de/research/mombasa/mse.html` [165].

In the *MOMBASA SE* the following functionalities have been implemented:

- Addressing and routing based on IP- and IP-style multicast,
- Multicast proxies in access points to disburden the mobile host from multicast group management,
- Advertisements/solicitations to advertise the availability of MEPs,
- Inter-MEP advertisements to register mobile hosts in advance,
- Support for different handover types: soft, predictive, inter-technology (vertical) handover,
- Support for different schemes for handover initiation (advertisement-based handover trigger and link-layer handover trigger)
- Differentiation between active and inactive mobile hosts, multicast-based paging to locate inactive mobile hosts,
- Buffering of data packets for predictive handover and paging,
- Policies to control system behavior (handover type, selection of optimal interface among multiple possible, control buffering, forwarding algorithm and paging algorithm).

Moreover, the implementation has the following features:

- The implementation supports IP (Version 4).
- It utilizes existing IP or IP-style multicast to support hard, soft and predictive handover.
- Neither does it require any modifications to the multicast routing protocol nor does it depend on a certain one.

- It supports heterogeneous networks, namely all technologies that support and are supported by IP. It has support for multiple network interfaces simultaneously in the mobile host (potentially of different technologies), and allows handover between access points on different interfaces and therefore handover between different technologies (vertical or inter-technology handover).
- The correspondent (i.e. fixed) host is not modified. That means any IP capable host can communicate with the mobile host. Only the mobile host and the access network require mobility-specific preparations.
- The system is soft state, i.e. a state is frequently be refreshed and times out otherwise. Soft state makes the system robust against the breakdown of network links and the crash of components within the system.
- The *MOMBASA SE* can be used for experimental evaluation of different algorithms for handover, location management including paging, buffer and forwarding strategies. It eases the implementation of advanced schemes by using policies to control system behavior.
- The *MOMBASA SE* provides a generic interface to the multicast protocol. Therefore it can be easily extended to support other multicast schemes.

The software platform has been implemented for Linux, a free Unix-type operating system [68, 103]. The main components of the *MOMBASA Software Environment* are implemented as daemons running in user space with root privileges. Additionally, some modifications to the Linux kernel were necessary.

The *MOMBASA SE* is comprised of the following main components:

Mobile Agent. The Mobile Agent is responsible for last-hop-signaling (detection of MEP, registration, handover) and idle detection on the mobile host.

Mobility Enabling Proxy. The Mobility Enabling Proxy (MEP) resides on the access point and is responsible for last-hop-signaling (advertisements, handling of registrations), administration of registered mobile hosts, inter-MEP-signaling (advertisement of registered mobile hosts to pre-register them at neighboring MEPs), MEP-GWP-signaling (sending of *Paging Updates*, handling of *Paging Requests*) and to execute multicast-operations (create, destroy subscribe, un-subscribe multicast groups).

Gateway Proxy. The GWP is executed in the gateway, maintains a paging table, and controls the paging of mobile hosts. If the used multicast protocol applies bi-directional multicast and/or closed multicast groups, as in the case study MB-CMAP, the gateway executes also multicast-operations.

NAT from/to multicast. Packets must be translated from unicast to multicast in the gateway and back to unicast in the access points. However, the original NAT code in the Linux kernel did not support translation between unicast and multicast realm. Thus, a patch had to be developed.

Kernel paging support. Paging in the gateway was implemented in the kernel.

The remaining sections are structured as follows: In the next section (Sect. 7.1) the implementation environment is described. In section 7.2 the design of the agents is presented and in Sect. 7.3 the extensibility of the *MOMBASA SE* is discussed.

7.1. Implementation Environment

The *MOMBASA SE* is implemented for a Linux system running on an x86 architecture (e.g. Intel Pentium, Pentium II, AMD Athlon). It can be easily ported to other architectures. For example, it was tested with the *StrongARM* processors [151], an up-to-date solution for portable communications and consumer electronic devices. The platform is implemented for Linux kernel version 2.2 and 2.4. If network address translation (NAT) between unicast and multicast is employed, the necessary kernel patch requires Linux kernel version 2.2. The *MOMBASA SE* uses only standard C and C++ libraries (including the Standard Template Library).

The *MOMBASA SE* was developed with a Linux installation based on the S.u.S.E. Linux distribution. However, since only standard libraries and tools (GNU tools) are used, the implementation can be used with any Linux distribution providing the necessary kernel and library versions.

The *MOMBASA SE* provides a generic interface to the multicast and therefore does not depend on a specific multicast type. The platform has been implemented using the following multicast protocols:

IGMPv2/PIM-SM. The multicast support is provided by the standard Linux kernel (IGMPv2 and kernel support for a PIM-SM Version 2 daemon) and a free multicast routing daemon for PIM-SM (pimd-2.1.0-alpha28) by the University of Southern California's Computer Networks and Distributed Systems Research Laboratory [120].

CMAP/CMNP The implementation of these multicast protocols are part of the Washington University Gigabit Switch Kit developed by the Applied Research Laboratory at the Washington University St. Louis. This kit comprises open, non-proprietary experimental networking equipment in hardware and software targeted for research purposes and includes a signaling protocol stack with CMAP/CMNP.

In addition, the platform is prepared for PIM-SSM multicast using IGMPv3.

7.2. Implementation Design

The three agents Mobile Agent, Mobility Enabling Proxy and Gateway Proxy have the same common design. In spite of the object-oriented implementation approach there is no inheritance relation between the agents and only the design of the agents is reused. The *MOMBASA SE* employs mainly two design patterns or design concepts:

- All agents are implemented as singletons, i.e. only one instance of the agent class may exist per application. This is ensured by making the constructor protected, thus no instances can be constructed from outside the scope of the agent. A protected static member variable holds a reference to the only agent instance. The instance can be retrieved by a public static method.
- The agents employ an event driven concept. Two types of events exist: external and internal events. External events are the reception of protocol messages. Internal events are the expiration of timers.

The design that is common to all agents can be seen in Fig. 7.1 by means of an Unified Modeling Language (UML) class diagram. Members or classes that are set in italics are placeholders for members and classes in the particular agents that have similar purposes but differ in some details. For example, the member *handle_XXX* represents the handler *handle_MEP_Advert* in the Mobile

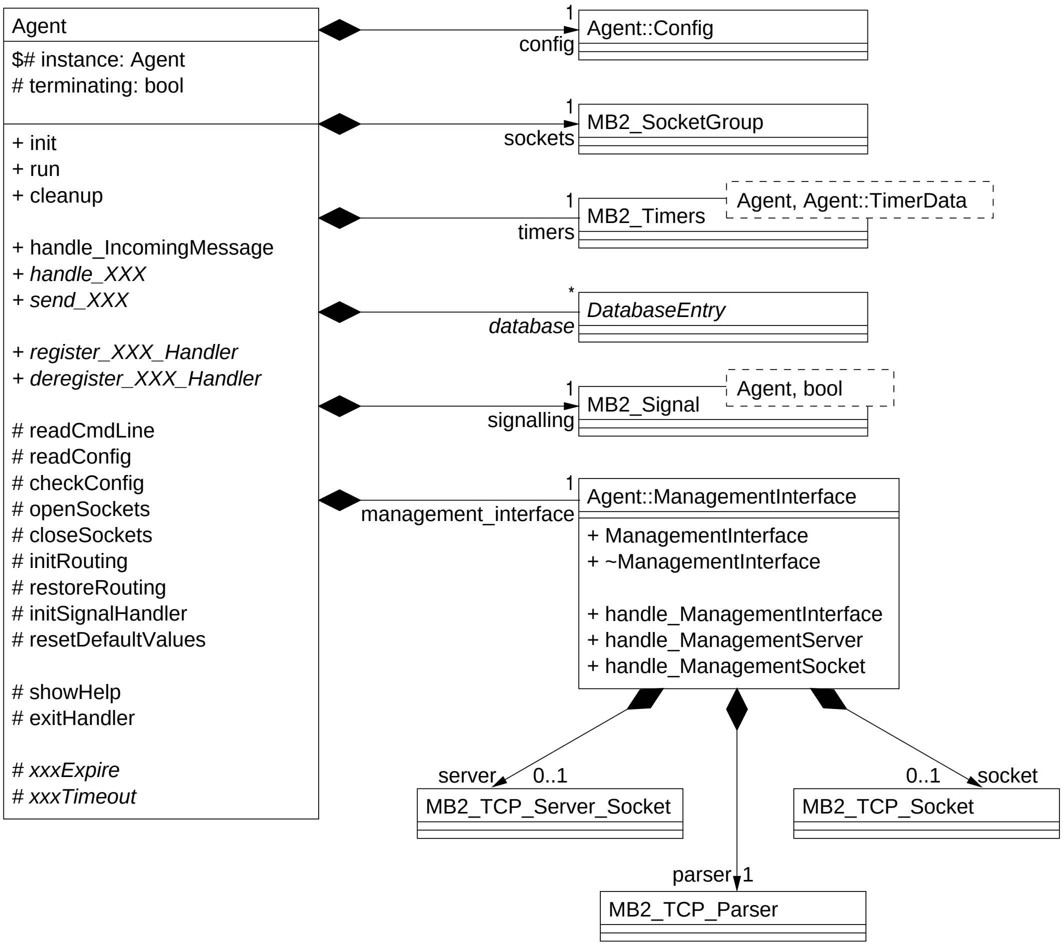


Figure 7.1.: Class diagram: Design of agents

Agent as well as other message and timer handlers in all agents. The detailed implementation design of each agent can be found in [164, 166].

A number of implementation issues are worth explaining:

Policies Handling of messages, selection of access point in the Mobile Agent, buffering and flushing buffers can be fine-tuned by policies. A policy is represented by a template class that has methods for pre- and post-processing. Policies can be registered and de-registered. Appropriate methods for each type of policy handler are provided by the agent class. In most cases multiple handlers can be registered for one message. Two phases exist for message processing. Preprocessing handlers are called before the standard message processing, post-processors are called afterwards (Fig. 7.2). Exceptions to this rule are the policy to select the access point *SelectBS* in the Mobile Agent and the buffer and flush policies. Only a single one of these handlers may be registered, and they have only a single phase.

The following exemplary policy illustrates the easiness of implementation.

```
PROCEDURE EagerHandover(access_point_list)
   newest_creation_time = -1;
   newest_feasible_access_point = NULL;
   FOR EACH  access_point_entry IN access_point_list
      IF NOT access_point_entry.stale AND NOT access_point_entry.busy  THEN
         IF access_point_entry.creation_time > newest_creation_time THEN
            newest_creation_time = access_point_entry.creation_time;
            newest_feasible_access_point = access_point_entry;
         END IF
      END IF
   END
   RETURN newest_feasible_access_point;
END PROCEDURE
```

The pseudo code represents the implementation of a policy for eager handover. It is executed in the Mobile Agent and determines the optimal access point among multiple possible access points: The access point that has sent the most recent advertisement is chosen as the next candidate access point the mobile host will register with.

Idle Detection in the MA One essential property of the mobile host is the distinction between the active and the inactive mode. The mobile host has to switch from active to the inactive mode after a configurable idle period (no IP data traffic). The idle detection works as follows: A packet socket is opened that receives all incoming and outgoing packets of the host. A socket filter is attached to that socket which only accepts IP data packets but rejects non-IP, signaling and broadcast packets, is attached to the socket. In the active mode the so-called idle thread does nothing but observe the packet socket and recording the timestamp of the last data packet. The main thread sets a timer to the duration of the activity timeout. When the timer expires, the timestamp of the last data packet is checked. If it lies within the last timer period the timer will be prolongated, otherwise the mobile host will switch to the inactive mode. The change from inactive to active mode is triggered by the reception of an incoming or outgoing packet by the idle thread or by a *PAGING_REQUEST*. In the case of outgoing data the packets are buffered by the idle thread until a valid registration at an access point can be obtained. To cause outgoing packets to appear on the idle socket but not be sent out on an interface a dummy device is used, a software network device which discards any packets. In the inactive mode the default route points to this device.

Buffering of packets in the MEP When a mobile is registered indirectly, packets for the mobile are buffered by this MEP to reduce loss of packets when the mobile executes a handover to this MEP. Each mobile entry has its own buffer, its own raw socket and its own buffer thread. The socket is attached to a filter accepting packets only for this mobile host. The buffer thread runs in an infinite loop and is canceled by the main thread either when the mobile entry becomes invalid or the mobile host becomes directly registered. In the latter case a flush thread is started to forward buffered data to the mobile host.

Buffering of packets in the GW During paging a mobile host it is not yet reachable and its exact position is not yet known. Thus, the data for the mobile host has to be buffered in the gateway proxy. Each mobile entry has its own buffer and all data packets arrive at the gateway through one special raw socket, the paging socket. Moreover, buffering is done by the main thread.

This is acceptable because the time period for which buffering is necessary is relatively short and so buffering will not be necessary for a lot of mobile hosts at the same time. As in the MEP flushing is done by a separate thread to avoid interruption of message processing.

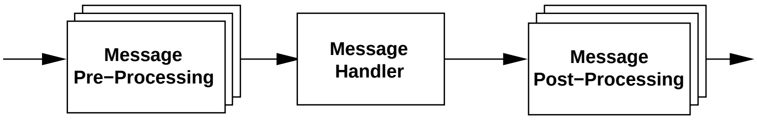


Figure 7.2.: Policy handling

7.3. Extensibility of the MOMBASA Software Environment

The software was designed to be expandable in a flexible and easy manner. This includes features for utilization of other multicast service models and protocols, implementation of enhanced features for mobility support, portability, configuration and testing.

Support for Multiple Multicast Service Models and Protocols. MOMBASA SE provides a generic interface to the multicast. Using this interface, the multicast is regarded as an abstract service for multicast group creation and destruction, multicast group subscribe and un-subscribe operations, packet delivery and operations to retrieve the members of a multicast group. This facilitates the examination of multicast types that offers interesting features for mobility support (such as third party signaling, etc. as in the case study MB-CMAP) without being limited to IGMPv2/v3 as a multicast group management protocol. In order to utilize a new multicast scheme in MOMBASA SE, the virtual methods of the generic interface class must be re-implemented

Implementation of Enhanced Features for Mobility Support. The *MOMBASA SE* has a clear design, detailed documentation about specification [59] exists, and it has been extensively tested [167]. Therefore, enhanced features can be easily implemented. Moreover, certain system behavior can be controlled and fine-tuned by policies. The software provides hooks for policy handler

- to control time and destination of handover,
- to control buffering and flushing of packets, and
- to retrieve signal quality for handover trigger.

These policy hooks are provided at various positions and hence, the *MOMBASA SE* ensures that enhanced algorithms can be easily implemented without redesigning major parts. Typical examples for extensions are buffering and flushing strategies and paging algorithms.

Portability. In the *MOMBASA SE* only standard libraries are used. This facilitates porting *MOMBASA SE* to other architectures. In particular, it is feasible to port *MOMBASA SE* to hand-held PC architectures running with a Linux operating system, e.g. mobile devices (such as Compaq's IPAQ).

Configuration and Testing. The software is instrumented with capabilities for easy configuration. Management interfaces offer debugging facilities at configurable levels. The implementation has been instrumented with testing facilities (such as accessing the actual state, access to databases, etc.). Test suites for automated testing are included in the source code distribution.

7.4. Summary

The *MOMBASA SE* is a software platform for investigation of multicast-based mobility support. It implements mobility-related functionalities augmenting existing multicast schemes. Together with multicast protocols these functionalities are assembled to a software environment for multicast-based mobility support in all-IP cellular networks. The *MOMBASA SE* already offers a rich set of functionalities. Nevertheless it is designed to be extended. Since IP and IP-style multicast are the subject of growing research efforts, this software environment facilitates the investigation of multicast-based mobility support using available and future multicast approaches and enhanced mobility mechanisms. In this thesis *MOMBASA SE* is used to create software prototypes for experimentation with selected case studies.

8. Evaluation of the Selected Case Studies

In the previous chapters a set of design principles for multicast-based mobility support has been developed and a network architecture as well as a set of protocols for four case studies have been designed. In this chapter the selected case studies are evaluated and the results compared.

The discussion of the general methodology in Chapt. 5 has been resulted in the decision for a measurement and analytical technique for evaluation, and, consequently, in the development of a software platform and prototypes for the case studies. The following sections describe the evaluation environment and present the results of the performance evaluation.

8.1. Measurement Environment

In general, the evaluation environment consists of hard- and software components and tools for load generation, WAN emulation, monitoring, and data analysis. In order to evaluate the case studies in a comparable environment, the network topology of the testbed setup as well as the tools for load generation, monitoring and data analysis are the same. The high-level network topology common to all case studies derived from the scenario has already been described in Fig. 5.7 in Sect. 5.2. In the next sections the specific measurement environment for each case study is shown.

It is common to all experimental setups that the wireless link is replaced by standard Ethernet. The advantage is the fact that the impact of an error-prone wireless channel on the performance metrics can be neglected. A manageable Ethernet hub interconnects the mobile host with the access points. The connectivity between the mobile host and the access points can be controlled by switching certain ports of the hub on and off, respectively. This technique allows to trigger a handover and to emulate the spatial coverage of wireless cells. Two scenarios are considered: In the *horizontal handover* scenario the mobile host uses a single Ethernet Network Interface Card (NIC). In the case of overlapping wireless cells the mobile host is connected to both access points for a short time. In the case of gaps in the coverage the mobile host is connected neither to the old nor to the new access points for the duration of time where the mobile host is located within the spatial gap. In the *vertical handover scenario* three Ethernet NICs are used in the mobile host (NIC A, B, and C). NIC C is dedicated to control the manageable hub. NIC B is interconnected with one of the access points (AP 1), and NIC C with the other access point (AP 2). Assuming that the hub ports for NIC B and AP 1 are switched on, a vertical handover is executed by switching off these ports and switching on the ports for NIC C and AP 2.

The following tools are used as part of the common evaluation environment:

Netperf. For load generation and data analysis, *Netperf* [117] is used. *NetPerf* is a network benchmark tool, that is commonly employed to measure various aspects of networking, such as bulk data transfer and response time. *NetPerf* consists of two parts: the *NetPerf* client and the server. When the *NetPerf* client is executed with appropriate configuration options, the *NetPerf* server is invoked automatically. A control connection is established between client and server, that is used to pass configuration information and results to and from the remote host.

Once the control connection is established and the configuration information has been passed, a separate data flow is opened using either UDP or TCP as a transport protocol.

Tcpdump. For traffic monitoring, in particular for tracing of TCP connections, *tcpdump* [124] was used. *Tcpdump* is a tool that allows to capture and dump network packets in order to make statistical analysis out of those traces. *Tcpdump* makes use of the packet capture library *libpcap* [125].

Tcptrace. For data analysis, the tool *tcptrace* [124] was applied. The purpose of *tcptrace* is to analyze TCP dump files (and other formats). It produces different types of output containing information on each connection seen such as elapsed time, bytes and segments sent and received, retransmissions, round trip times, window advertisements, throughput, and more. In combination with *xplot* [146], *tcptrace* can also generate a number of graphs for further analysis.

Softlink. For emulation of WAN links with high delays, the tool *softlink* [141] was used. *Softlink* filters outgoing IP packets and can execute certain, pre-configured operations with these packets. It is capable to limit the bandwidth of a certain physical link, to emulate the latency, packet drop rate, packet ordering, and link outages. *Softlink* is implemented for the Linux operating system as a virtual device that attaches to a physical device.

NET-SNMP. The tool *NET-SNMP* [118] implements a software agent that facilitates the exchange of management information between network devices based on the *Simple Network Management Protocol (SNMP).* The tool was used to control the manageable Ethernet hub in order to trigger handover.

Evaluation scripts. A set of *perl*-based scripts [39] were developed to extract handover specific information from tcpdump-files in order to estimate handover latency and packet loss of a handover.

As it will be detailed below, the network nodes in the testbeds execute the Linux operating system. In general, the Linux default setting for network protocol parameters are used, except the minimal routing cache flushing delay is set to zero in order to make the routing table changes immediately. The need of specific kernel patches are stated accordingly.

8.1.1. Measurement Environment for the Case Study MB-ASM

The measurements for the case study MB-ASM were conducted using the setup in Fig. 8.1.[1] The access network consists of a single mobile host, two access points and two multicast routers, whereas one of the routers is dedicated as a gateway. The WAN representing the Internet consists of a dedicated router (denoted by WAN emulator) and a correspondent host. All nodes are based on standard Pentium-class personal computers equipped with 128 MByte RAM each. The network interface cards (NICs) are standard 10Mbps Ethernet devices. The multicast router and the access points, as well as the gateway and the multicast router are connected back-to-back by dedicated 10Mbps 10BaseT Ethernet. The other network nodes are interconnected by a standard 10BaseT Ethernet hub. The mobile host is equipped and interconnected as described above.

The setup consists of an IP class A network (10.) as the WAN and multiple class C networks (192.168.) as the access network. In particular, each wireless cell represents an IP class C network. When the mobile host executes a handover, it changes between the IP networks 192.168.10. and 192.168.20.

[1] The dashed circle in Fig. 8.1 and in the figures for the other setups mark the main differences.

The following software is installed: In all network nodes the Linux operating system, kernel version 2.2.x is installed. The mobile host, access points, and the gateway execute the appropriate instances of the *MOMBASA Software Environment* (see Chapt. 7). The access points provide the multicast support as provided by the standard Linux kernel version 2.2 (IGMPv2 and kernel support for PIM-SM). The multicast router and the gateway execute a multicast routing daemon for PIM-SM (pimd-2.1.0-alpha28) by the University of Southern California's Computer Networks and Distributed Systems Research Laboratory (see [120]). Address translation from IP unicast and multicast addresses and vice versa in gateway and access points is provided by a Linux kernel patch being part of the *MOMBASA Software Environment*.

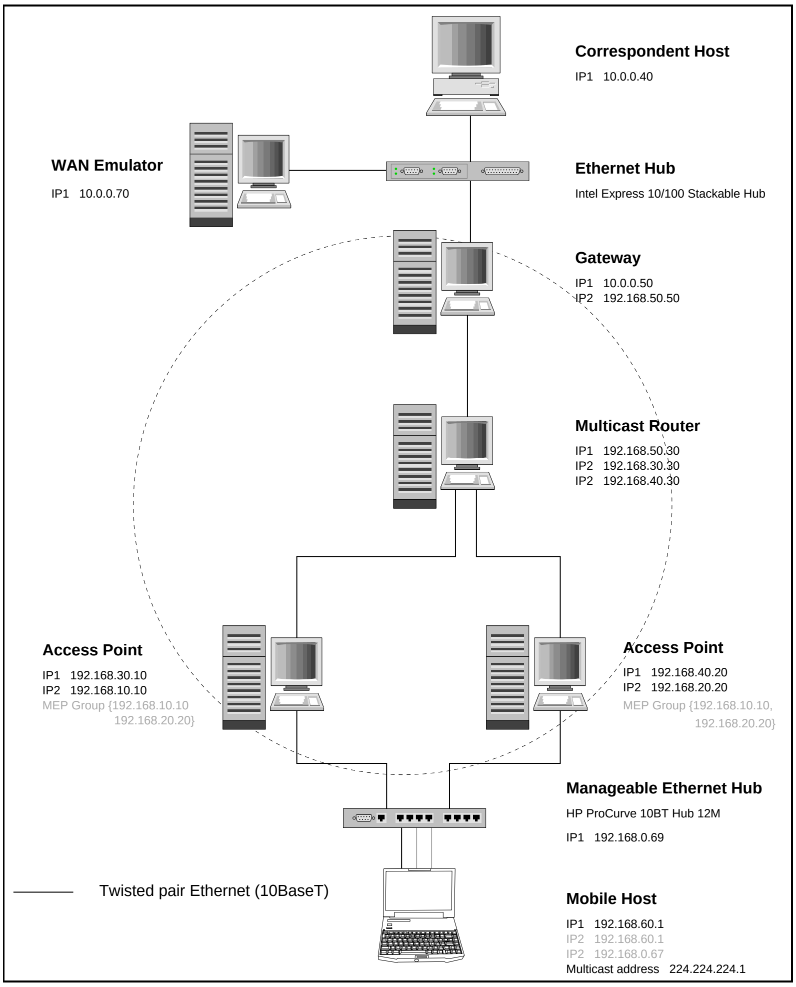
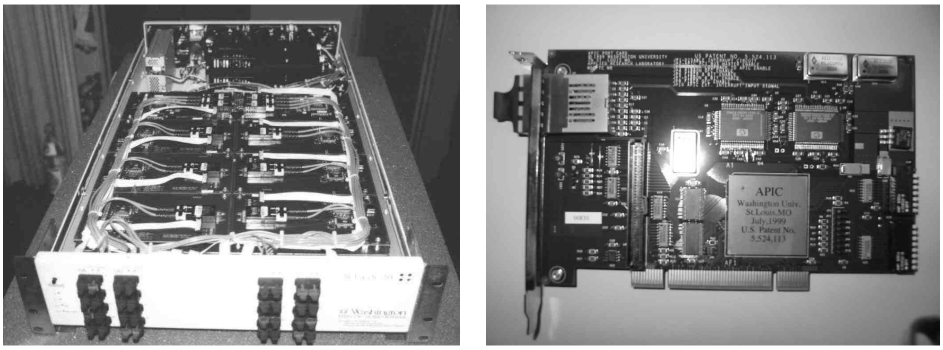


Figure 8.1.: Testbed setup for the case study MB-ASM

8.1.2. Measurement Environment for the Case Study MB-CMAP

The measurement environment for the case study MB-CMAP consists of an access network (mobile host, two access points, cell switch, switch controller and gateway) and the emulated WAN (correspondent host, WAN emulator) (Fig. 8.3). The core of the access network is the Washington University Gigabit Switch (WUGS), a cell switch that interconnects the gateway with the access points. The cell switch belongs to the *Washington University Gigabit Switch Kit* – a kit of experimental network equipment for research purposes [119]. The switch is a remote-controlled, 8 port cell switch with an open, non-proprietary, well-documented architecture supporting up to 2.4 Gbps. An important feature of the cell switch is the efficient support of multicast by means of a technique termed *cell-recycling*: In order to efficiently duplicate cells, the switching fabric of the cell switch can forward a cell to an output port and optionally recycle back to an input port. In a switch with a buffered multi-stage switching network this method yields optimal scaling to the switching network complexity and the amount of routing memory required [28].

The cell switch is interconnected by fiber to the access points (OC-3 [61]) and to the gateway and the switch controller (HP Glink). In addition to the 10BaseT Ethernet NICs, the access points are equipped with an ATM Port Interconnect Controller (APIC) network interface card, another key hardware component of the *Washington University Gigabit Switch Kit.* An *APIC* NIC is based on a customized IC that is basically a $2x2$ cell switch operating at 1.2Gbps following the UTOPIA interface specification. The APIC provides a number of up-to-date features, such as segmentation and reassembly of AAL 5 frames directly to and from the host's memory, eliminating the need for large amounts of memory on the network interface card, zero-copy data transfers using virtual memory page re-mapping techniques and direct user-level control of the APIC in a fully secure fashion [48].



(a) Cell Switch

(b) APIC-based NIC

Figure 8.2.: Core hardware components of the *Washington University Gigabit Switch Kit* [119]

The gateway and the switch controller are equipped with a ENI-155p NIC. In addition, the gateway has a 10BaseT Ethernet NIC for interconnection with the other part of the testbed.

The IP network structure for the setup of the case study MB-CMAP consists of an IP class A network (10.) as the WAN and multiple class C networks (192.168.) as the access network. Again, each wireless cell represents an IP class C network and forces a network-layer handover of the mobile host. Unlike the setup of the case study MB-ASM, the access network consists of a single IP class C network (wireless cells not included). This 192.168.0. network represents a CLIP Logical IP Subnet (LIS).

The operating system used in the testbed is Linux 2.4.18 including the APIC device drivers[2] for the access points and Linux 2.2.18 for the other nodes. In the gateway and switch controller the *ATM-on-Linux* software distribution (atm-0.59) [6] is installed.

In the testbed, the appropriate instances of the *MOMBASA Software Environment* are installed, whereas the MEPs in the access points and the *Gateway Proxy* in the gateway include extensions for the support of CMAP multicast operations. These extensions are part of the version 2.0 of the *MOMBASA Software Distribution* [165].

The switch controller executes the necessary protocol stack to control the cell switch. The software includes a CMAP Session Manager (CMAP SM), a CMAP Connection Manager (CMAP CM), and a switch controller (Gigabit Switch Controller (GBNSC)) (see [56] for details of the switch controller protocol setup).

For the investigation of multicast-based mobility support the implementation of the CMAP/CMNP protocol stack was modified. The modifications include the addition of CMAP operations (*Trace_Call* and *Trace_Ep* operation), as well as modifications of other operations (*Open_Call* and others) to allow the setting of attributes for the traceability of calls and endpoints. It is noted that the modifications are based on the specification of CMAP, but were not included in the installed software distribution.

In addition to the extensions of the CMAP source code, the inter-process communication between the instances of the protocol stack was optimized. The instances use TCP for inter-process communication. It was observed that multiple TCP segments were needed to exchange a single signaling message. With the optimization only a single TCP segment is used resulting in a much less duration of time for the CMAP operations. Details of the optimization can be found in [14].

8.1.3. Simulation Environment for the Case Study MIP-SGM

The evaluation technique for the MIP-SGM is based on simulation. The selected simulation tool is the *network simulator (ns)-2* [52]. *ns-2* is a discrete event simulator, written in C++ with an OTCL interpreter as a front end. *ns-2* already includes a set of simulation models, such as for TCP and routing, and is continuously extended with contributions by researchers. For the performance evaluation of the case study MIP-SGM routing extensions for non ad-hoc routing (NOAH) [168] and extensions of Mobile IP and hierarchical Mobile IP to *ns-2* from the *COMET* research group at *Columbia University* as part of the *Columbia University Micro-Mobility Suite (CIMS)* [26] were used. In order to conduct experiments with comparable parameters as in the measurement environments, a few modifications of the CIMS implementation of Mobile IP and hierarchical Mobile IP were necessary. These modifications include mainly policies for handover trigger. The modified version allows a validation of the simulation model with results from the conducted measurements (see Appendix B).

Based on the modified implementation *ns-2* has been extended to support small group multicast (SGM) and the protocol operations of the case study MIP-SGM (see the description in 6.2). The SGM module for *ns-2* introduces a new packet header type with a multi-destination option in the IP header and a new classifier entity that provides the routing of packets with multiple destinations. In addition to the SGM module, the Mobile IP source code has been extended to support simultaneous bindings in the home agent (for basic Mobile IP) and in the switching foreign agent (for hierarchical Mobile IP). Details of the implementation can be found in [95].

Fig. 8.5 and 8.6 show the simulation setup for basic Mobile IP and hierarchical Mobile IP as *nam*–screen-shots and their logical topology.[3] In principal, the IP structure of the simulated network is the same as in the measurement environment of the reference case that will be described in the

[2] Available at `http://www.arl.wustl.edu/gigabitkits/`

[3] *nam* (Network Animator) is an animation tool for viewing network simulation traces and part of *ns-2*.

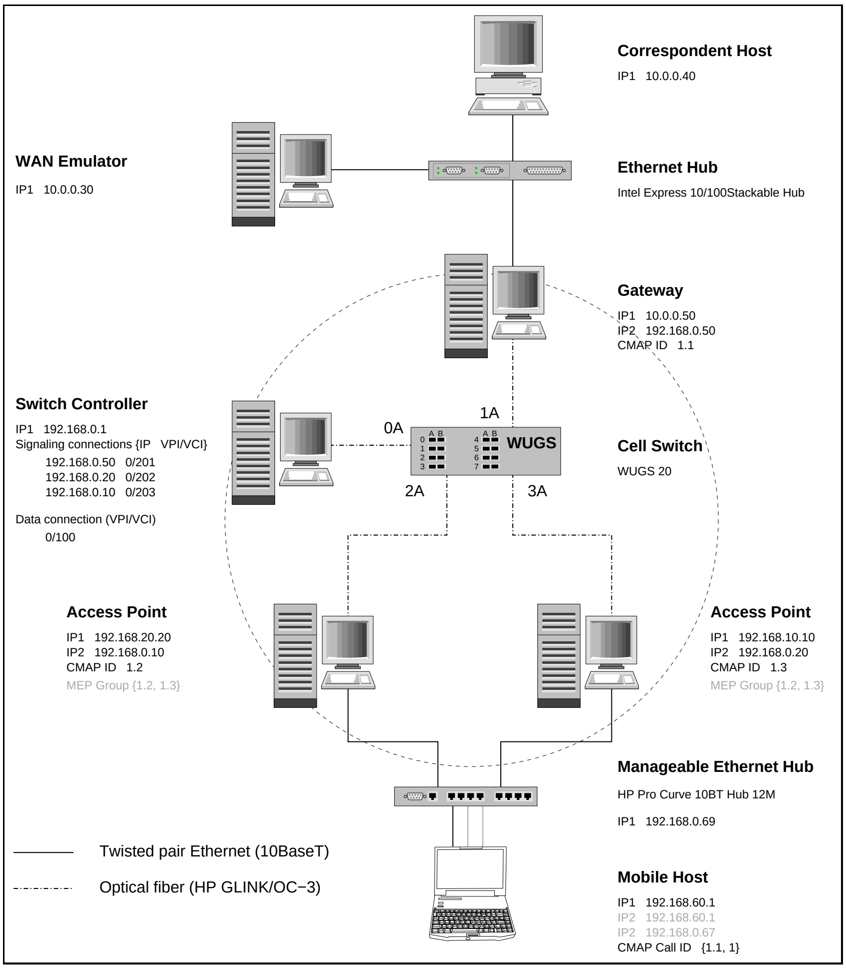


Figure 8.3.: Testbed setup for the case study MB-CMAP

next section: The topology consists of multiple IP networks, where the wireless cells represent own networks in the IP sense.

8.1.4. Measurement Environment for the Reference Case Basic and Hierarchical Mobile IP

The main hardware components of the experimental environment for the basic and hierarchical Mobile IP are a correspondent host, a WAN emulator, a mobile host, two access points, and three routers (Fig. 8.7 and 8.8). One of the routers is dedicated as the Mobile IP home agent, another as the WAN emulator. In the setup for hierarchical Mobile IP (Fig. 8.8) a second router acts as a highest foreign agent. The IP structure of the setup is based on an IP class A network (10.) as the WAN and multiple IP class C networks as the access network. Each network node (routers and access points) in the access network interconnects two IP class C networks.

The operation system of the network nodes is Linux kernel version 2.2.18. In the home agent the

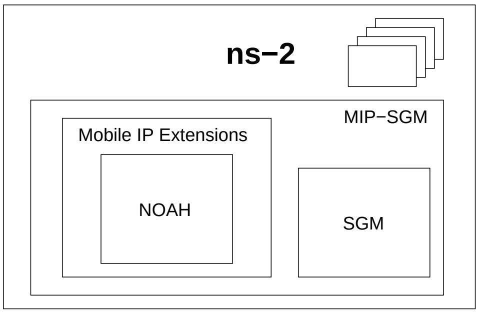
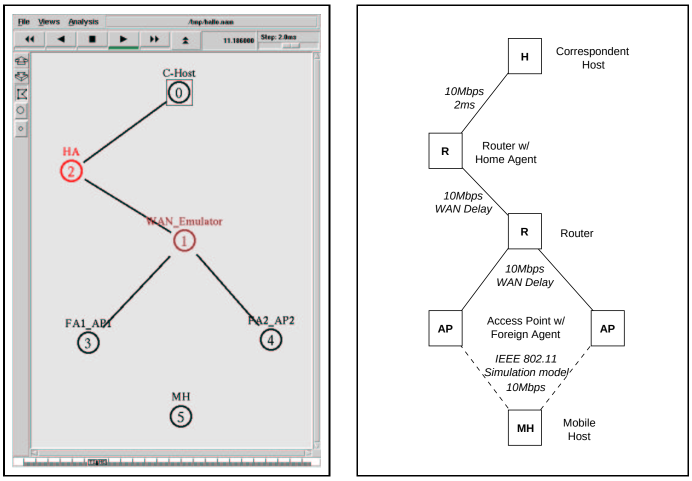


Figure 8.4.: Extensions of the simulation tools ns-2 for the case study MIP-SGM

Redhat Linux distribution 6.1 [137] is used, in all other network nodes the SuSE Linux distribution 6.2 [152] is installed.

The Mobile IP software is the *Dynamics* implementation of Mobile IP [62, 63, 121], version 0.6.2. The implementation includes support for hierarchical foreign agents. The Mobile IP instances are implemented as *demons* running in user space. In its basic version the Dynamics implementation is fully RFC 2002 [129] compliant. The implementation has been modified to enable the foreign agent to send advertisements at a higher frequency than once per second.[4] In the basic Mobile IP setup (Fig. 8.7) the mobile host executes the *Dynamics* Mobile Agent, the access points execute the *Dynamics* Foreign Agents, and the router runs the *Dynamics* Home Agent. In the setup for hierarchical Mobile IP (Fig. 8.8) the router in the center also executes a *Dynamics* foreign agent (highest foreign agent). All foreign agents are configured to form a hierarchy with the router as the highest foreign agent and the access points as lowest foreign agents. For handover between the lowest foreign agents the highest foreign agent becomes the switching foreign agent. The home agent is not involved.

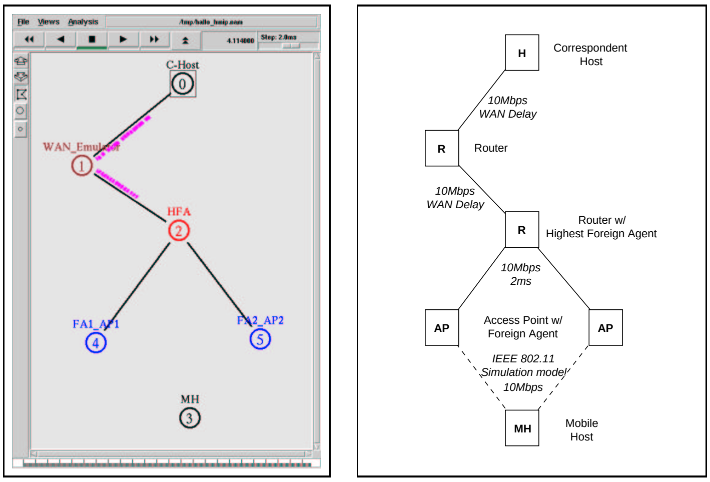
[4] Consequently, the lifetime unit of the advertisements was changed to a unit of milliseconds (instead of seconds) as well as the timing of the mobile host demon that can count the advertisement lifetime and trigger handovers at a milliseconds time scale. However, the maximum advertisement frequency is once per 10 ms due to the timer granularity of the Linux operating system.



(a) *nam* screenshot

(b) Logical topology

Figure 8.5.: Simulation setup for SGM-enhanced Mobile IP



(a) *nam* screenshot

(b) Logical topology

Figure 8.6.: Simulation setup for SGM-enhanced hierarchical Mobile IP

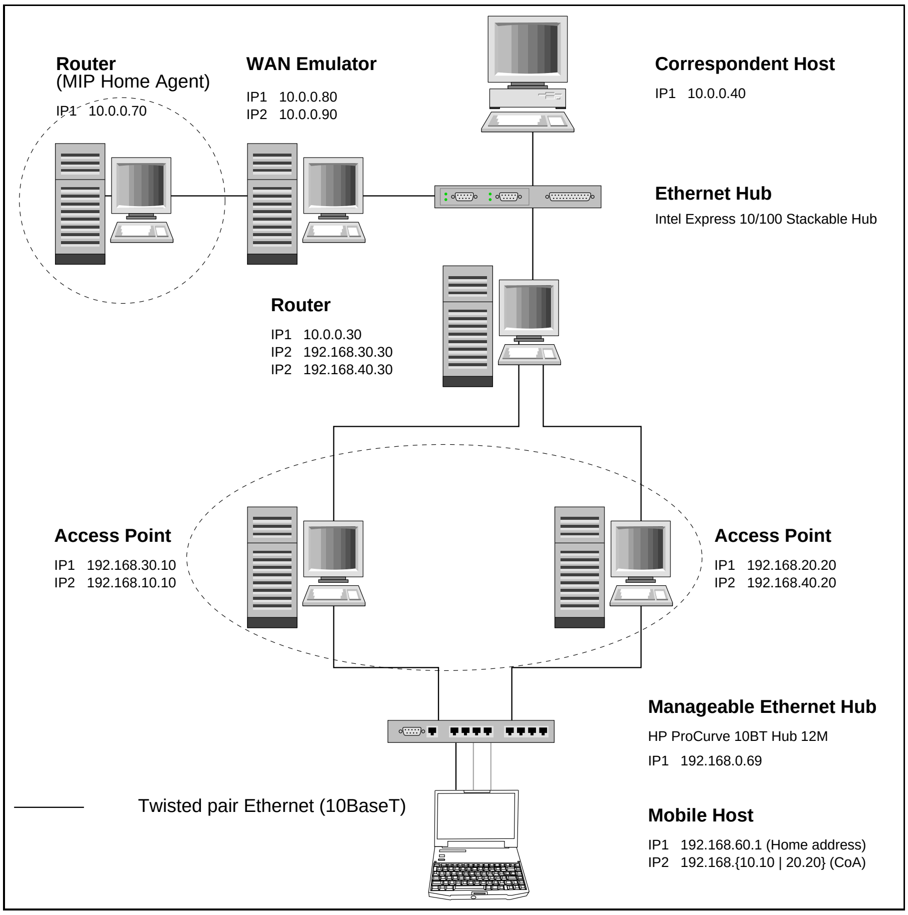


Figure 8.7.: Testbed setup for the reference case basic Mobile IP

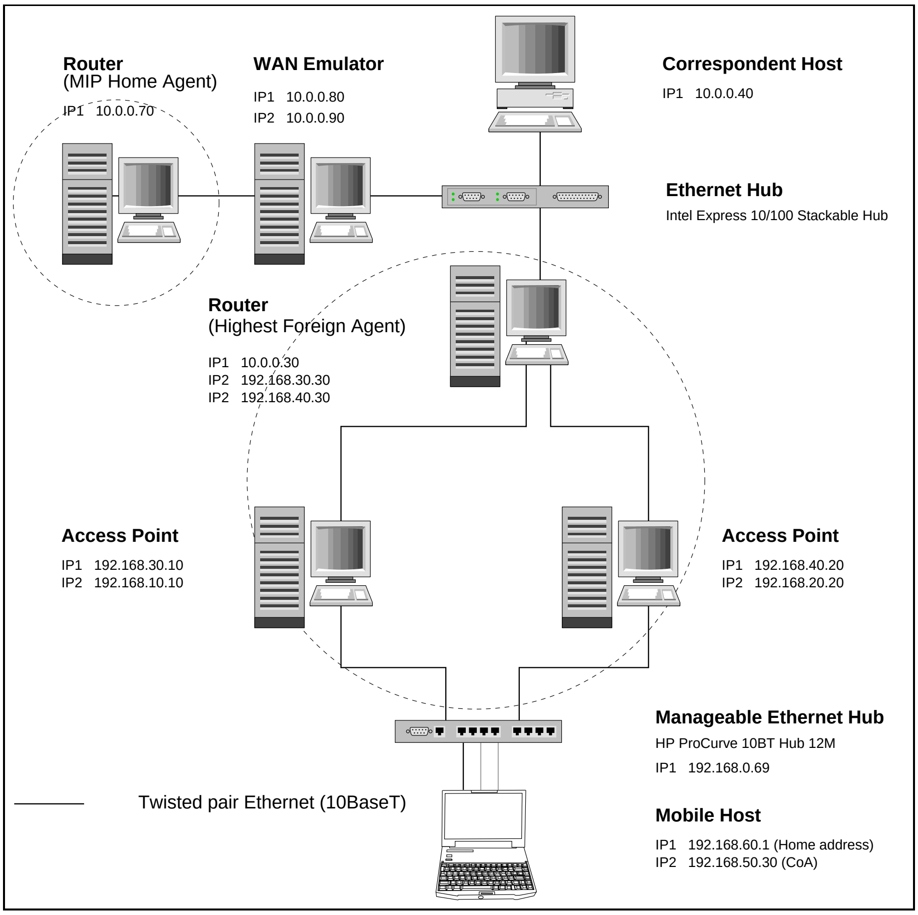


Figure 8.8.: Testbed setup for the reference case hierarchical Mobile IP

8.2. Performance Results for the Reference Case Basic and Hierarchical Mobile IP

In this section the handover performance for the reference case basic and hierarchical Mobile IP is presented. The results are the basis for the performance comparison with the case studies. In addition, the performance results will be used to validate the simulation results of the case study MIP-SGM.

8.2.1. Handover Latency

In Fig. 8.9 the handover latency $T_{\text{HO\_Lat}}$ of basic Mobile IP (Fig. 8.9(a)) and hierarchical Mobile IP (Fig. 8.9(b)) for advertisement-based trigger is drawn. First, the measurement results are given. Then, the analysis is presented and the numerical results are compared with those from the measurements.

The experiments were conducted using the parameters listed in Tab. 8.1.[5]

In basic Mobile IP the delay between the mobile host and the home network/correspondent host has a strong impact on the handover latency. Therefore, in this experiment the round trip time (RTT) between the mobile host and the correspondent host is varied from 20 ms to 420 ms. This was achieved by changing the WAN delay parameter in the range from 0 ms to 100 ms in the WAN emulator in the setup (Fig. 8.7 and 8.8). Since reverse tunneling instead of triangular routing is applied, an IP packet from the correspondent host to the mobile host is delayed twice by the WAN emulator (see Fig. 8.7 and 8.8). Hence, for a given value of the *WAN emulation* parameter T_{Delay}, the overall RTT amounts to more than $4 * T_{\text{Delay}}$.

In Fig. 8.9(a) and 8.9(b) the measurement graphs show the mean handover latency for about 230 handovers. For Mobile IP the handover latency grows linearly from about 380 ms to about 570 ms. For hierarchical Mobile IP the handover latency remains constant at about 360 ms.

In order to validate the measurement results, the handover latency can be decomposed into the duration to detect the handover $T_{\text{HO\_Detect}}$ and to execute the handover $T_{\text{HO\_Exec}}$:

$$T_{\text{HO\_Lat}} = T_{\text{HO\_Detect}} + T_{\text{HO\_Exec}} \tag{8.1}$$

For advertisement-based trigger $T_{\text{HO\_Detect}}$ can be expressed by

$$\begin{aligned} T_{\text{HO\_Detect, lower bound}} &= T_{\text{Advert\_Lt}} - \frac{1}{r_{\text{Advert}}} = \frac{2}{r_{\text{Advert}}} && (8.2) \\ T_{\text{HO\_Detect, upper bound}} &= T_{\text{Advert\_Lt}} + T_{\text{Advert\_Defer,Max}} + T_{\text{Mov}} \\ &= \frac{3}{r_{\text{Advert}}} + T_{\text{Advert\_Defer,Max}} + T_{\text{Mov}} && (8.3) \end{aligned}$$

with the following variables:

T_{Mov}	Duration of mobile host's physical movement from one wireless to another [ms]
r_{Advert}	Advertisement rate $\left[\frac{1}{s}\right]$,
T_{Advert_Lt}	Lifetime of an advertisement; set to $\frac{3}{r_{\text{Advert}}}$ [ms],
$T_{Advert\_Defer,Max}$	Maximum duration of the advertisement deferral.

[5] The experiments were conducted for advertisement-based trigger only. Although the *Dynamics* Mobile IP implementation [121] provides support for link-layer trigger, its usage requires wireless network interface cards. Since in the setup the wireless links were replaced by Ethernet, this feature could not be used.

Notation	**Value**
Traffic type	UDP
Direction of traffic flow	Downlink
Packet size [Bytes]	1024
Packet burst size [N]	1
Inter-burst time [ms]	10
Mean value of exponential CDT distribution [s]	10
Offset ϵ [s]	5
Overlap of cells [s]	0
WAN delay [ms]	0,10,20,30,40,50,100
FA Advertisement interval [s]	0.1
FA Advertisement lifetime [s]	0.3
Re-registration interval [s]	10
Registration lifetime [s]	30
Handover initiation policy	Advertisement-based trigger
Handover type	Horizontal; vertical
Tunnel lifetime [s]	600 s
Tunneling type	Reverse tunneling
Foreign agent packet capsulation	Enabled (No co-located FA)
Registration error reply interval	10
Test length [min]	60

Table 8.1.: Basic and hierarchical Mobile IP: Measurement parameters

In the *Dynamics* Mobile IP implementation an advertisement is deferred by a random interval between 0 and $T_{\text{Advert\_Defer,Max}}$

$T_{\text{HO\_Exec}}$ for basic Mobile IP can be expressed by

$$\begin{aligned} T_{\text{HO\_Exec}} &= 2T_{\text{Proc,MH}} + T_{\text{RegReq,MH} \rightarrow \text{FA}} + T_{\text{Proc,FA}} + T_{\text{RegReq,FA} \rightarrow \text{HA}} \\ &\quad + T_{\text{Proc,HA}} + T_{\text{RegRepl,HA} \rightarrow \text{FA}} + T_{\text{Proc,FA}} + T_{\text{RegRepl,FA} \rightarrow \text{MH}} \end{aligned} \tag{8.4}$$

and for hierarchical Mobile IP

$$\begin{aligned} T_{\text{HO\_Exec}} &= 2T_{\text{Proc,MH}} + T_{\text{RegReq,MH} \rightarrow \text{LFA}} + T_{\text{Proc,LFA}} + T_{\text{RegReq,LFA} \rightarrow \text{HFA}} \\ &\quad + T_{\text{Proc,HFA}} + T_{\text{RegRepl,HFA} \rightarrow \text{LFA}} + T_{\text{Proc,LFA}} + T_{\text{RegRepl,LFA} \rightarrow \text{MH}} \end{aligned} \tag{8.5}$$

with

$T_{\textit{Proc,Node}}$	Duration of message processing in a *node*, where MH stands for mobile, host, FA for foreign agent, LFA and HFA for lowest and highest foreign agent, respectively, and HA for home agent,
$T_{\textit{RegReq,Node A} \rightarrow \textit{Node B}}$	Duration for the transmission of a *Registration Request* message from *Node A* to *Node B*, where *Node A* or *Node B* can be FA (Foreign Agent), LFA (Lowest Foreign Agent), HFA (Highest Foreign Agent), and HA (Home Agent),
$T_{\textit{RegRepl,Node A} \rightarrow \textit{Node B}}$	Duration for the transmission of a *Registration Reply* message from *Node A* to *Node B*, with the same meaning for *Node A* and *Node B* as above,
$T_{\textit{RegRepl,Node A} \rightarrow \textit{Node B}}$	Duration for the transmission of a *Registration Reply* message from *Node A* to *Node B*, where *Node A* and *Node B* stand for HA, FA, LFA, HFA, and HA, respectively.

For simplification it is assumed that

$$\mathbf{T}_{\text{Proc}} = T_{\text{Proc,MH}} = T_{\text{Proc,FA}} = T_{\text{Proc,LFA}} = T_{\text{Proc,HFA}} = T_{\text{Proc,HA}} \tag{8.6}$$

and

$$\begin{aligned}
\mathbf{T}_{\text{Msg}} &= T_{\text{Advert}} = T_{\text{Solicit}} \\
&= T_{\text{RegReq,MH} \rightarrow \text{FA}} = T_{\text{RegRepl,FA} \rightarrow \text{MH}} && (8.7)\\
&= T_{\text{RegReq,MH} \rightarrow \text{LFA}} = T_{\text{RegRepl,LFA} \rightarrow \text{MH}} \\
&= T_{\text{RegRepl,HFA} \rightarrow \text{LFA}} = T_{\text{RegReq,LFA} \rightarrow \text{HFA}} && (8.8)
\end{aligned}$$

Eq. (8.7) does not include $T_{\text{RegRepl,FA} \rightarrow \text{HA}}$ and $T_{\text{RegRepl,HA} \rightarrow \text{FA}}$. However, both terms can be equated:

$$T_{\text{RegReq,FA} \rightarrow \text{HA}} = T_{\text{RegRepl,HA} \rightarrow \text{FA}} \tag{8.9}$$

The resulting equations for $T_{\text{HO\_Lat}}$ are summarized in Tab. 8.2. Comparing the measurement results and numerical results from the analysis, the 99 % confidence interval of the mean handover latency is between the lower and upper bound (LB and UB) of the analysis.

		Advertisement-based trigger
Basic Mobile IP	LB	$5T_{\text{Proc}} + 2T_{\text{Msg}} + 2T_{\text{RegReq,FA} \rightarrow \text{HA}} + \frac{2}{r_{\text{Advert}}}$
	UB	$5T_{\text{Proc}} + 2T_{\text{Msg}} + 2T_{\text{RegReq,FA} \rightarrow \text{HA}} + T_{\text{Mov}} + T_{\text{Advert\_Defer,Max}} + \frac{3}{r_{\text{Advert}}}$
Hierarchical Mobile IP	LB	$5T_{\text{Proc}} + 4T_{\text{Msg}} + \frac{2}{r_{\text{Advert}}}$
	UB	$5T_{\text{Proc}} + 4T_{\text{Msg}} + T_{\text{Mov}} + T_{\text{Advert\_Defer,Max}} + \frac{3}{r_{\text{Advert}}}$

Table 8.2.: Basic and hierarchical Mobile IP: Analysis of the handover latency

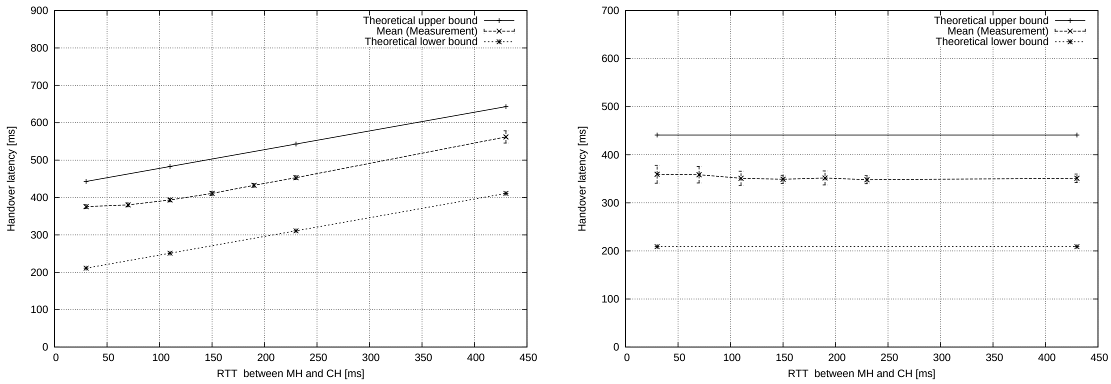
Fig. 8.10 compares the handover latency of vertical and horizontal handover for a RTT of 120ms (mean and standard deviation of the handover latency for about 230 handovers). In comparison

Notation	**Value**
T_{Msg}	1 ms
r_{Advert}	$10\frac{1}{s}$
T_{Proc}	1 ms
$T_{RegReq,FA \rightarrow HA}$	2 ms, 22 ms, 52 ms, 102 ms
T_{Mov}	90-130 ms
$T_{Advert\_Defer,Max}$	2 ms

Table 8.3.: Basic and hierarchical Mobile IP: Variable settings in the analytical evaluation of the handover latency

		Advertisement-based trigger
Basic	LB	207 ms + $2T_{\mathrm{RegReq,FA} \rightarrow \mathrm{HA}}$
Mobile IP	UB	439 ms + $2T_{\mathrm{RegReq,FA} \rightarrow \mathrm{HA}}$
Hierarchical	LB	209 ms
Mobile IP	UB	441 ms

Table 8.4.: Basic and hierarchical Mobile IP: Numerical results for the analysis of the handover latency

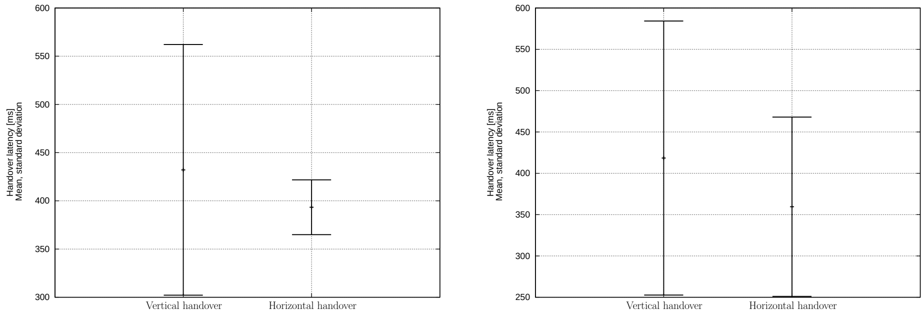


(a) Basic Mobile IP

(b) Hierarchical Mobile IP

Figure 8.9.: Basic and hierarchical Mobile IP: Handover latency versus RTT between CH and MH (Advertisement-based trigger)

to the horizontal handover, the mean handover latency for vertical handover is increased by the duration for switching off/on the additional ports of the manageable hub in the experimental setup. The measurement results show that a vertical handover within the access network has no considerable impact on the handover latency since the observed differences are caused by the experimental setup.



(a) Basic Mobile IP

(b) Hierarchical Mobile IP

Figure 8.10.: Basic and hierarchical Mobile IP: Comparison of the handover latency versus RTT between CH and MH for vertical and horizontal handover (Advertisement-based trigger)

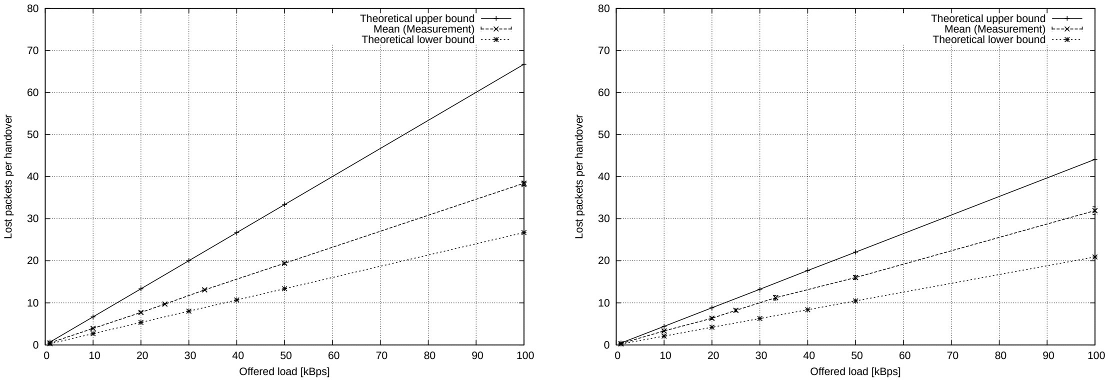
8.2.2. Packet Loss and Duplication

In Fig. 8.11 the packet loss L_{HO} of basic and hierarchical Mobile IP for advertisement-based trigger is shown. The figures include the results from the measurements and the analysis.

The experiments were conducted using the same parameters as in Tab. 8.1, but with a fixed RTT between the mobile host and the correspondent host of 100 ms. Also, the offered load was varied from 1 $\frac{kB}{s}$ to 100 $\frac{kB}{s}$ (1 to 100$\frac{\text{packets}}{s}$ with a constant packet size of 1 kB). For basic Mobile IP the measurement graph of L_{HO} in Fig. 8.11(a) grows linearly up to 39 packets per handover for an offered load of 100 kBps. For hierarchical Mobile IP (Fig. 8.11(b)) the packet loss increases to about 32 packets for the same offered load. A duplication of packets was not observed ($D_{HO} = 0$).

The theoretical packet loss for a constant data rate can simply be calculated by Eq. (8.10). Using the numerical results for the handover latency $T_{\text{HO\_Lat}}$ calculated in Sect. 8.2.1 gives the numerical results for L_{HO} listed in Tab. 8.5.

$$L_{HO} = N_{\text{Lost,HO}} = T_{\text{HO\_Lat}} r_{\text{Data}} \qquad (8.10)$$



(a) Mobile IP

(b) Hierarchical Mobile IP

Figure 8.11.: Basic and hierarchical Mobile IP: Packet loss versus offered load (Advertisement-based trigger)

		Advertisement-based trigger
Basic	LB	$(0.207 + 2T_{\text{RegReq,FA} \rightarrow \text{HA}}) * r_{\text{Data}}$ pkts
Mobile IP	UB	$(0.439 + 2T_{\text{RegReq,FA} \rightarrow \text{HA}}) * r_{\text{Data}}$ pkts
Hierarchical	LB	$0.209 * r_{\text{Data}}$ pkts
Mobile IP	UB	$0.441 * r_{\text{Data}}$ pkts

Table 8.5.: Basic and hierarchical Mobile IP: Numerical results for the analysis of the packet loss

8.2.3. Relative TCP Throughput

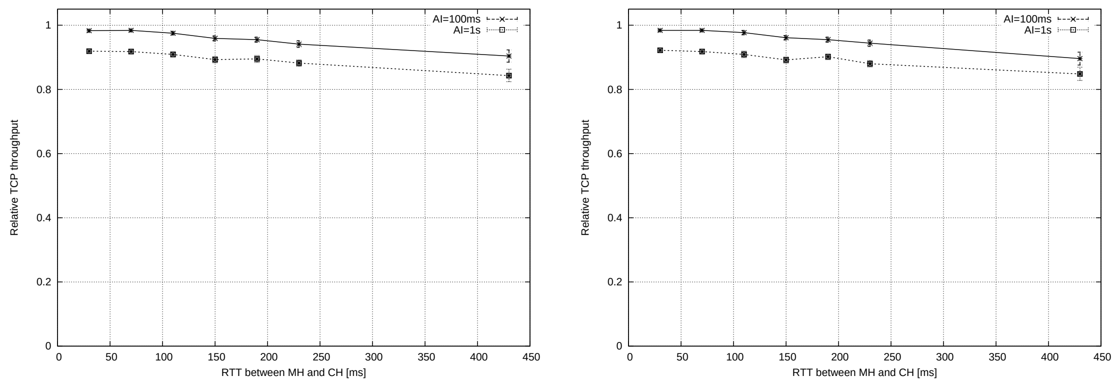
The relative TCP throughput B_{Rel} of basic and hierarchical Mobile IP for a short-lived TCP connection with a single handover and a long-lived TCP connection with multiple handovers is shown in Fig. 8.12 and Fig. 8.13, respectively.

The experiments were conducted with the parameters in Tab. 8.1. In the first experiment with short-lived TCP connections the duration of a connection was set to 60 s and the RTT was varied from 30 ms to 230ms. The resulting relative TCP throughput is averaged over 100 measured values of the TCP throughput.

In the second experiment the handover frequency was varied from 0 (no handover) to about 6 $\frac{\text{handover}}{\text{min}}$ by setting the *mean cell dwell time* parameter (Tab. 8.1). The RTT between the mobile host and the correspondent host was set to 130ms and remained constant. In order to observe the impact of multiple handovers on TCP, where the handover events impact each other, a single long-lived TCP connection with subsequently executed handover events for each value of the *cell dwell time* was observed. The duration of a measurement was adapted to the handover frequency: For rare handover events the duration of a measurement was increased, i.e. 9 hours for a handover frequency of 0.6 $\frac{\text{handover}}{\text{min}}$.

For a short-lived TCP connection of 60 s and a single handover B_{Rel} of basic Mobile IP reduces to 0.9 for an advertisement interval of 100 ms and to 0.87 for an advertisement interval of 1s at a RTT of 430 ms (Fig. 8.12(a)). For hierarchical Mobile IP B_{Rel} is slightly better than that of basic Mobile IP.

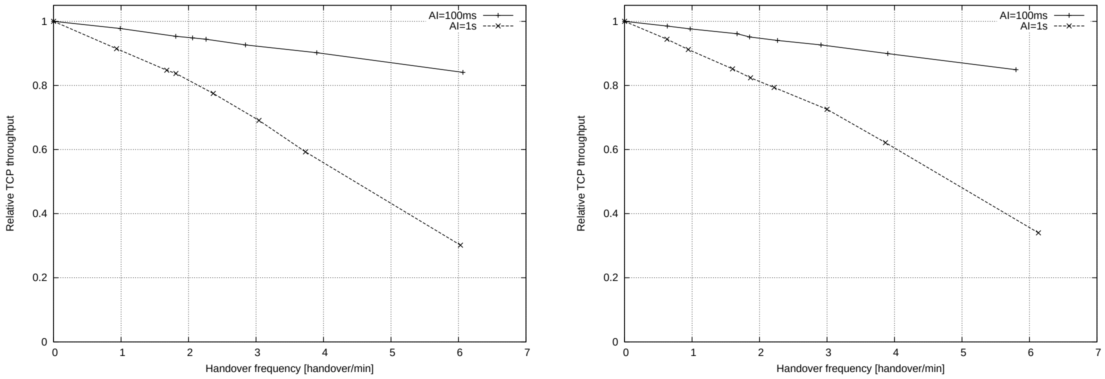
For a long-lived TCP connection with multiple handovers and advertisement-based trigger (advertisement interval of 100 ms) the relative TCP throughput of basic Mobile IP reduces to about 0.85 for a handover frequency of 6 $\frac{\text{handover}}{\text{min}}$ (Fig. 8.13(a)) and for hierarchical Mobile IP to about 0.83 (Fig. 8.13(b)). For an advertisement interval of 1 s the relative TCP throughput of basic Mobile IP degrades to about 0.32 at 6 $\frac{\text{handover}}{\text{min}}$(Fig. 8.13(a)). With the same advertisement interval the relative TCP throughput of hierarchical Mobile IP is slightly better and amounts to about 0.35 (Fig. 8.13(b)).



(a) Basic Mobile IP

(b) Hierarchical Mobile IP

Figure 8.12.: Basic and hierarchical Mobile IP: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover (Advertisement-based trigger)



(a) Basic Mobile IP

(b) Hierarchical Mobile IP

Figure 8.13.: Basic and hierarchical Mobile IP: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers (Advertisement-based trigger)

8.3. Performance Results for the Case Study MB-ASM

In this section the handover performance for the case study MB-ASM is evaluated by means of measurements and analysis. The measurements were conducted in the testbed setup described in Sect. 8.1.1. The theoretical results of the analysis will be used to validate the measurement results.

8.3.1. Handover Latency

In Fig. 8.17 the handover latency $T_{\text{HO\_Lat}}$ of soft and predictive horizontal handover for advertisement-based trigger (Fig. 8.17(a) and 8.17(c)) and link-layer trigger (Fig. 8.17(b) and 8.17(d)) is plotted. The figures contain measurement results as well as theoretical results. First, the measurement results are given. Then, the analysis is presented and numerical results from analysis are compared with the measurement results. The performance of vertical handover is given at the end of the section.

The experiments were conducted using the parameters listed in Tab. 8.6. Similar to the measurement procedure for the reference case Mobile IP, the RTT between the mobile host and the correspondent host is varied from 20 ms to 420 ms by setting the WAN delay parameter in the WAN emulator (Fig. 8.1). In Fig. 8.17 each point in the measurement graphs is obtained by averaging the handover latency over about 230 handovers (see the estimation of the number of handover events for a measurement duration of 1 hour in Fig. 5.10). The graphs of the measurement in Fig. 8.17(a) – 8.17(d) remain constant over the RTT, it can be concluded that the handover latency is independent of the round-trip time between the correspondent host and the mobile host. This observation is in accordance with the expectation: In the multicast handover scheme the rerouting node for handover is close to the mobile. In the selected setup the rerouting node is directly connected to both access points. The mean handover latency for soft handover amounts to about 150 ms (link-layer trigger) and 180 ms (advertisement-based trigger). For predictive handover the measured values are about 120 ms (link-layer trigger) and 270 ms (advertisement-based trigger). In the case of soft handover, a relatively high number of outliers could be observed. For soft handover with advertisement-based trigger 90 % of the measured values were smaller than 220 ms (90 % percentile as drawn in Fig. 8.17(a)) and 99 % of the values are below 1 s (99 % percentile, not shown in Fig. 8.17(a)). The outliers cause a left-skewed distribution of the handover latency and clearly impact the mean value. The reason of the outliers are specific to the implementation of the used multicast routing demon, more precisely the interaction between user and kernel space.

In order to validate the measurement results, the handover latency is analyzed. Fig. 8.14 – 8.16 illustrate the analysis of soft handover for advertisement-based trigger – with eager and lazy detection, respectively – and with link-layer trigger.[6] The figure depicts events appearing during a handover in the mobile host and assigns appropriate variables to the fractions of time contributing to the overall handover latency. While the figure addresses the soft handover case, the illustration can be used as a basis for the predictive handover case as well.

The handover latency can be decomposed into the duration to detect the handover $T_{\text{HO\_Detect}}$ and to execute the handover $T_{\text{HO\_Exec}}$, as shown in Eq. (8.1) for the Mobile IP reference case.

For advertisement-based trigger and soft handover $T_{\text{HO\_Detect}}$ can be expressed as

$$\begin{aligned} T_{\text{HO\_Detect, soft, lower bound}} &= T_{\text{Mov}} \\ T_{\text{HO\_Detect, soft, upper bound}} &= \frac{2}{r_{\text{Advert}}} + T_{\text{Mov}} \end{aligned} \tag{8.11}$$

[6] The dashed circles in the figures point to the differences between the schemes for handover detection.

Notation	**Value**
Traffic type	UDP
Direction of traffic flow	Downlink
Packet size [Bytes]	1024
Packet burst size [N]	1
Inter-burst time [ms]	10
Mean value of exponential CDT distribution [s]	10
Offset ϵ [s]	5
Overlap of cells [s]	0
WAN delay [ms]	0, 50, 100, 200, 400
MEP Advertisement interval [s]	0.1 (Advertisement-based trigger) 10 (Link-layer trigger)
MEP Advertisement lifetime [s]	0.3 (Advertisement-based trigger) 30 (Link-layer trigger)
Inter-MEP Advertisement interval [s]	0.1
Re-registration interval [s]	10
Registration lifetime [s]	30
Handover initiation policy	Advertisement-based trigger link-layer trigger
Handover execution policy	Soft, predictive
Handover type	Horizontal, vertical
Paging	Off
Address translation	NAT
Test length [min]	60

Table 8.6.: MB-ASM: Measurement parameters

and for advertisement-based trigger and predictive handover

$$\begin{aligned} T_{\text{HO\_Detect, predictive, lower bound}} &= T_{\text{Advert\_Lt}} - \tfrac{1}{r_{\text{Advert}}} &&= \frac{2}{r_{\text{Advert}}} \\ T_{\text{HO\_Detect, predictive, upper bound}} &= T_{\text{Advert\_Lt}} + T_{\text{Mov}} &&= \frac{3}{r_{\text{Advert}}} + T_{\text{Mov}} \end{aligned} \tag{8.12}$$

and for link-layer trigger (and both soft and predictive handover)

$$T_{\text{HO\_Detect, lower bound}} = T_{\text{Mov}} + T_{\text{Proc,MH}} + T_{\text{Solicit}} + T_{\text{Proc,MEP}} + T_{\text{Advert}} \tag{8.13}$$

$$T_{\text{HO\_Detect, upper bound}} = T_{\text{Mov}} + T_{\text{Proc,MH}} + T_{\text{Solicit}} + T_{\text{Proc,MEP}} + T_{\text{Advert}} \tag{8.14}$$

with the following variables:

T_{Mov} Duration of mobile host's physical movement from one wireless cell to another in the case of non-overlapping cells [ms],
$T_{Proc,MH}$ Duration of message processing in the mobile host [ms],
$T_{Proc,MEP}$ Duration of message processing in the MEP [ms],
$T_{Solicit}$ Duration for the transmission of a *MH_Solicitation* message,
r_{Advert} Advertisement rate $\left[\frac{1}{s}\right]$,
T_{Advert_Lt} Lifetime of an advertisement, set to $\frac{3}{r_{\text{Advert}}}$ [ms].

For soft handover $T_{\text{HO\_Exec}}$ is given by

$$T_{\text{HO\_Exec, lower bound}} = 2\ T_{\text{Proc,MH}} + T_{\text{RegReq}} + T_{\text{Proc,MEP}} + T_{\text{RegRepl}} \quad (8.15)$$

$$T_{\text{HO\_Exec, upper bound}} = T_{\text{Proc,MH}} + T_{\text{RegReq}} + T_{\text{Proc,MEP}} + T_{\text{IGMP\_Rep}} + 2T_{\text{Pkt}} \quad (8.16)$$

and for predictive handover by

$$T_{\text{HO\_Exec}} = 2T_{\text{Proc,MH}} + T_{\text{RegReq}} + T_{\text{Proc,MEP}} + T_{\text{RegRepl}} \quad (8.17)$$

with

T_{RegReq} Duration for the transmission of a *Registration Request* message,
$T_{RegRepl}$ Duration for the transmission of a *Registration Reply* message,
T_{IGMP_Rep} Duration for the transmission of an *Unsolicited IGMP Membership Report* message from the MEP to the multicast router,
T_{Pkt} Duration for the transmission of a data packet from the multicast router to the MEP, and from the MEP to the mobile host, respectively.

The lower bound of $T_{\text{HO\_Exec}}$ for soft handover is achieved when the MEP is still subscribed for the mobile host's multicast group and the mobile host attempts to register with this MEP. This case occurs when the access point still holds a registration for the mobile host that had executed a handover to another access point, and then the mobile host executes a handover back to the former access point. The upper bound of $T_{\text{HO\_Exec}}$ for soft handover is attained in the case if the MEP initially subscribes for the mobile host's multicast group when the mobile host registers.

Assuming that

$$T_{\text{Proc,MH}} = T_{\text{Proc,MEP}} = \mathbf{T}_{\text{Proc}} \quad (8.18)$$

and

$$T_{\text{Advert}} = T_{\text{Solicit}} = T_{\text{RegReq}} = T_{\text{RegRepl}} = T_{\text{Pkt}} = \mathbf{T}_{\text{Msg}} \quad (8.19)$$

yield the equations summarized in Tab. 8.7.

Using the variable settings listed in Tab. 8.8, the theoretical value of $T_{\text{HO\_Lat}}$ can be calculated. It is noted that the value of $T_{\text{IGMP\_Rep}}$ depends on the used implementation and may vary among different operation systems. Although the IGMP specification [55] demands to send an *Unsolicited IGMP Membership Report* immediately after the application's request to subscribe to the multicast group, many IGMP implementations defer sending an *Unsolicited IGMP Membership Report* by a small delay. The purpose of this delay is to avoid bursts of multicast subscription messages when many applications attempts to join a multicast group at the same time (for example after a power supply fault). In the Linux operating system installed in the testbed the variable that determines the

		Advertisement-based trigger	**Link-layer trigger**
Soft handover	LB	$3T_{\text{Proc}} + 2T_{\text{Msg}} + T_{\text{Mov}}$	$5T_{\text{Proc}} + 4T_{\text{Msg}} + T_{\text{Mov}}$
	UB	$2T_{\text{Proc}} + 3T_{\text{Msg}} + T_{\text{Mov}} + \frac{2}{r_{\text{Advert}}} + T_{\text{IGMP\_Rep}}$	$4T_{\text{Proc}} + 5T_{\text{Msg}} + T_{\text{Mov}} + T_{\text{IGMP\_Rep}}$
Predictive handover	LB	$3T_{\text{Proc}} + 2T_{\text{Msg}} + \frac{2}{r_{\text{Advert}}}$	$5T_{\text{Proc}} + 4T_{\text{Msg}} + T_{\text{Mov}}$
	UB	$3T_{\text{Proc}} + 2T_{\text{Msg}} + T_{\text{Mov}} + \frac{3}{r_{\text{Advert}}}$	$5T_{\text{Proc}} + 4T_{\text{Msg}} + T_{\text{Mov}}$

Table 8.7.: MB-ASM: Analytical results of the handover latency

deferral (*IGMP_Initial_Report_Delay*) was set to 1 and a resulting delay of maximum 10 ms between reception of a *Registration Request* message to sending of a *IGMP Membership Report* message was observed by measurements.[7] Moreover, the value of T_{Mov} is set to 90 ms and 130 ms (for the lower and upper bound, respectively). It corresponds with the delay introduced by the method to emulate a handover: As it was verified by measurements, the duration to switching off/on Ethernet ports of the manageable hub by means of SNMP takes a duration between 90 ms and 100 ms. Since two SNMP operations triggered by the mobile host are necessary, the delay was measured between sending the *SNMP Request* message of the first SNMP operation and receiving the *SNMP Response* message of the second SNMP operation in the mobile host.

Notation	**Value**
r_{Advert}	$\frac{10}{s}$
T_{IGMP_Rep}	10 ms
T_{Mov}	90–130 ms
T_{Msg}	1 ms
T_{Proc}	1 ms

Table 8.8.: MB-ASM: Variable settings in the analytical evaluation of the handover latency

The numerical results of the analysis of the handover latency are listed in Tab. 8.9. Comparing the measurement results with the theoretical results, the 99 % confidence interval of the mean $T_{\text{HO\_Lat}}$ lies between the theoretical lower and upper bound attained from the analysis.

Fig. 8.18 compares the handover latency for vertical and horizontal handover (mean with 99 % confidence interval). The mean handover latency for soft handover is about 130ms and for predictive handover about 80ms higher than for horizontal handover. The reason for the difference lies rather in the experimental setup: For vertical handover four SNMP operations are executed for controlling the ports of the hubs, whereas for horizontal handover only 2 operations are needed. The time needed for the additional operations is in the magnitude of the increased handover latency for vertical handover. Hence, it can be stated that for vertical handover the handover latency is not significant higher.

[7] It is noted that the used version of the Linux operating system had to be modified: Originally, the Linux kernel version 2.2.18 sets the variable *IGMP_Initial_Report_Delay* to value of $1 * HZ$ whereas HZ represents a system-specific variable. The value of the *IGMP_Initial_Report_Delay* results in a delay that is uniformly distributed between 0 and 1s. In subsequent versions (2.2.19 and later) *IGMP_Initial_Report_Delay* is set to 1. Since Linux

		Advertisement-based trigger	Link-layer trigger
Soft handover	LB	105 ms	99 ms
	UB	345 ms	149 ms
Predictive handover	LB	204 ms	100 ms
	UB	434 ms	140 ms

Table 8.9.: MB-ASM: Numerical results for the analysis of the handover latency

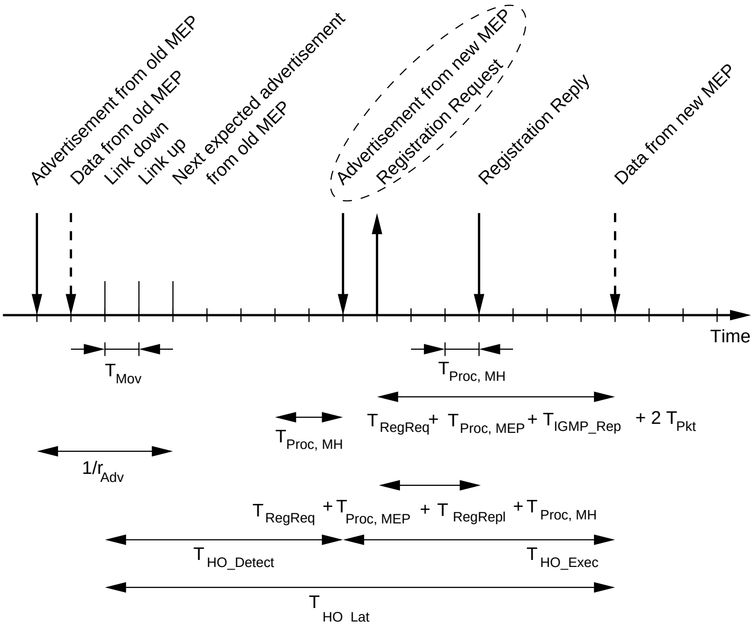

Advertisement from old MEP
Data from old MEP
Link down
Link up
Next expected advertisement from old MEP
Advertisement from new MEP
Registration Request
Registration Reply
Data from new MEP
Time
T_{Mov}
$T_{Proc, MH}$
$T_{RegReq} + T_{Proc, MEP} + T_{IGMP\_Rep} + 2\,T_{Pkt}$
$T_{Proc, MH}$
$1/r_{Adv}$
$T_{RegReq} + T_{Proc, MEP} + T_{RegRepl} + T_{Proc, MH}$
T_{HO_Detect}
T_{HO_Exec}
T_{HO_Lat}

Figure 8.14.: Illustration of the handover latency analysis with advertisement-based trigger (Eager detection)

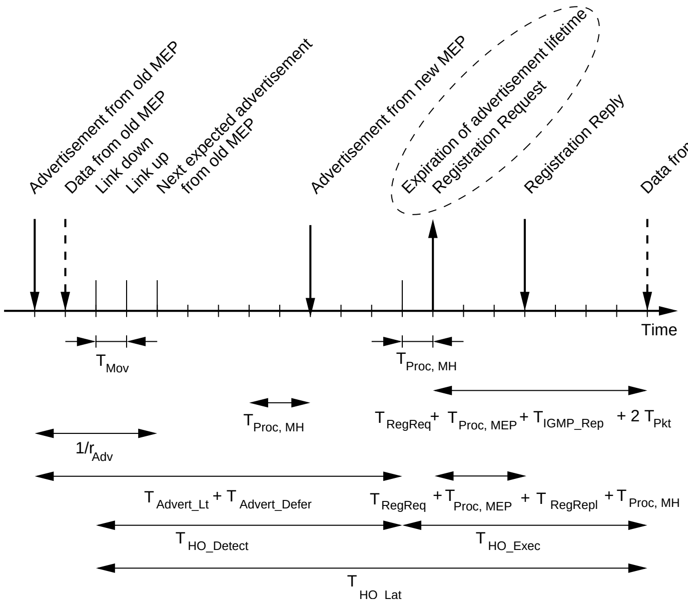

Advertisement from old MEP
Data from old MEP
Link down
Link up
Next expected advertisement from old MEP
Advertisement from new MEP
Expiration of advertisement lifetime
Registration Request
Registration Reply
Data from new MEP
Time
T_Mov
T_Proc, MH
T_Proc, MH
T_RegReq + T_Proc, MEP + T_IGMP_Rep + 2 T_Pkt
1/r_Adv
T_Advert_Lt + T_Advert_Defer
T_RegReq + T_Proc, MEP + T_RegRepl + T_Proc, MH
T_HO_Detect
T_HO_Exec
T_HO Lat

Figure 8.15.: Illustration of the the handover latency analysis with advertisement-based handover (Lazy detection)

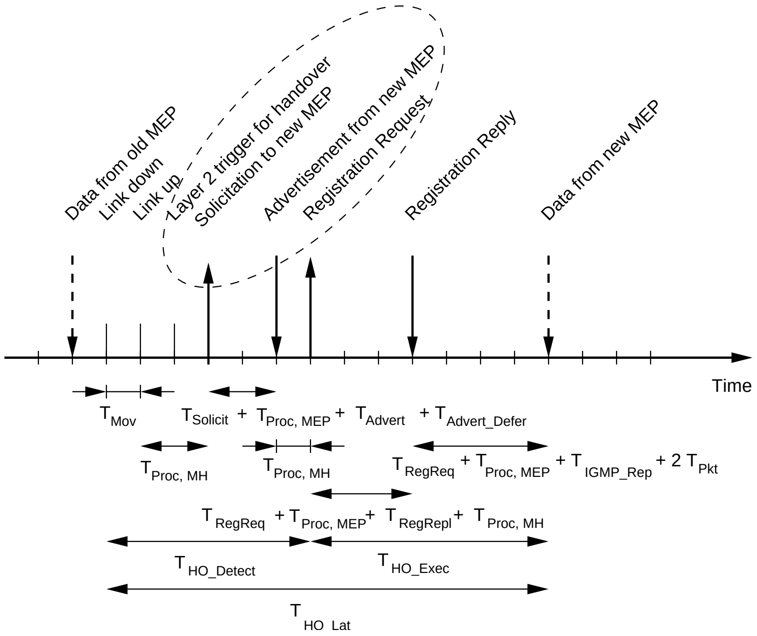
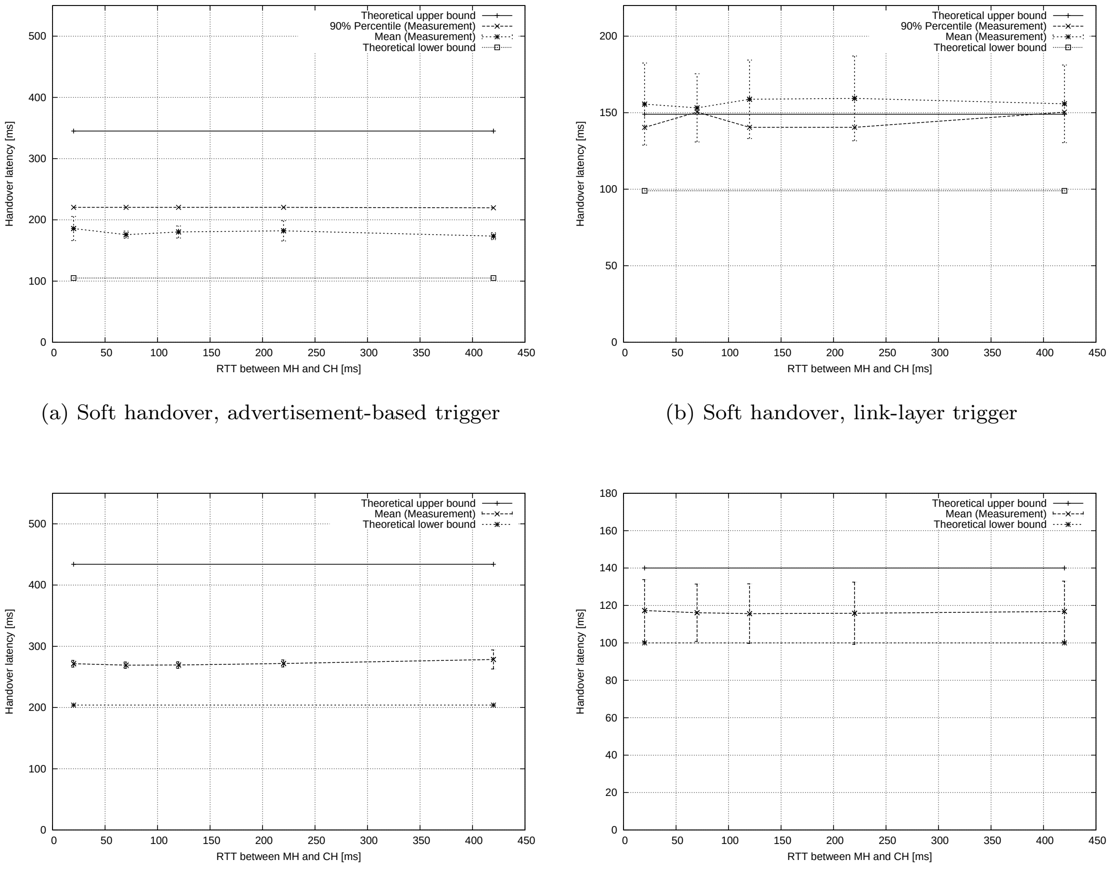

Data from old MEP
Link down
Link up
Layer 2 trigger for handover
Solicitation to new MEP
Advertisement from new MEP
Registration Request
Registration Reply
Data from new MEP
Time
T_Mov
T_Solicit + T_Proc, MEP + T_Advert + T_Advert_Defer
T_Proc, MH
T_Proc, MH
T_RegReq + T_Proc, MEP + T_IGMP_Rep + 2 T_Pkt
T_RegReq + T_Proc, MEP + T_RegRepl + T_Proc, MH
T_HO_Detect
T_HO_Exec
T_HO Lat

Figure 8.16.: Illustration of the the handover latency analysis with link-layer trigger



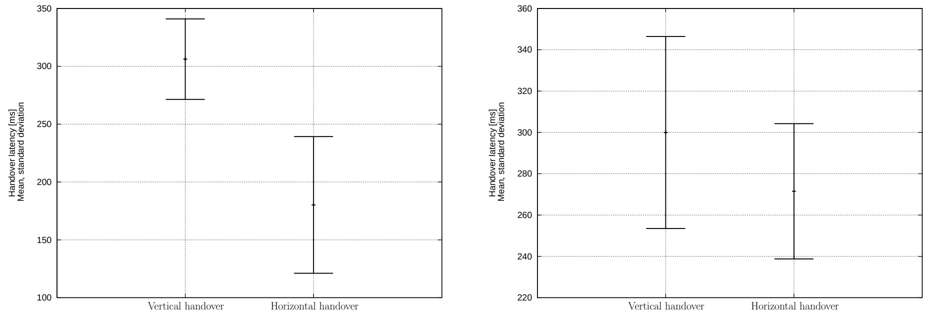
(a) Soft handover, advertisement-based trigger

(b) Soft handover, link-layer trigger

(c) Predictive handover, advertisement-based trigger

(d) Predictive handover, link-layer trigger

Figure 8.17.: MB-ASM: Handover latency versus RTT between CH and MH



(a) Soft handover

(b) Predictive handover

Figure 8.18.: MB-ASM: Comparison of the handover latency versus RTT between CH and MH for vertical and horizontal handover

8.3.2. Packet Loss and Duplication

In Fig. 8.19 and 8.20 the packet loss L_{HO} and the packet duplication D_{HO} for advertisement-based trigger and link-layer trigger are plotted. The figures include the results from the measurements and the analysis.

The experiments were conducted using the same parameters as in Tab. 8.6, but with a fixed RTT between the mobile host and the correspondent host of 100 ms. Also, the offered load was varied from 1 $\frac{kB}{s}$ to 100 $\frac{kB}{s}$ (1 to 100$\frac{\text{packets}}{s}$ with a constant packet size of 1 kB). The measurement graphs in Fig. 8.19(a) and 8.19(b) show the packet loss per handover L_{HO} averaged over about 230 handovers. For soft handover a linear dependence of the packet loss from the offered load exists. For soft handover with advertisement-based trigger (Fig. 8.19(a)) the packet loss increases up to 16 packets at a load of 100 $\frac{kB}{s}$, for link layer trigger (Fig. 8.19(b)) to 12 packets. The predictive handover ensures a reliable packet transport, i.e. no packets are lost.

The measurement results for the number of duplicated packets per handover D_{HO} versus the offered load are drawn in Fig. 8.20. For soft handover D_{HO} equals 0. For predictive handover and advertisement-based trigger D_{HO} grows up to offered load of about 80 $\frac{kB}{s}$ (80 $\frac{\text{packets}}{s}$ with a constant packet size of 1 kB) and then decreases slightly (Fig. 8.20(a)). The graph shows a similar behavior for predictive handover with link-layer trigger (Fig. 8.20(b)), but at a smaller absolute value.

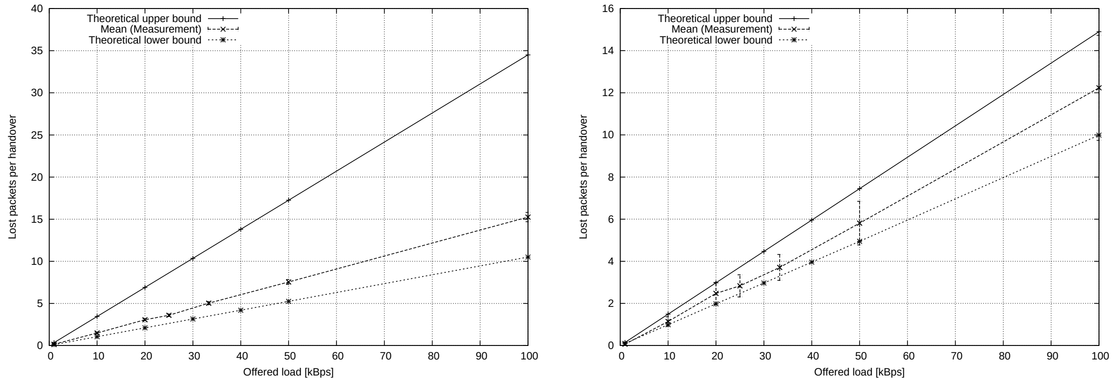
The theoretical packet loss per handover for downlink traffic is determined by the number of packets that the mobile host could not directly[8] receive during the handover process ($N_{\text{Lost,HO}}$) and the number of packets that are buffered and forwarded by the new access point to the mobile host when the mobile host registers with the new access point ($N_{\text{Forw,HO}}$):

$$L_{HO} = \begin{cases} N_{\text{Lost,HO}} - N_{\text{Forw,HO}} & \text{for } N_{\text{Lost,HO}} > N_{\text{Forw,HO}}, \\ 0 & \text{else.} \end{cases} \tag{8.20}$$

A negative loss can be regarded as a duplication of packets, however the conditions in Eq. (8.20)

version 2.2.18 had to be used due to other reasons, the value of *IGMP_Initial_Report_Delay* was fixed to 1.

[8] Without buffering and forwarding in the new access point.



(a) Soft handover, advertisement-based trigger

(b) Soft handover, link-layer trigger

Figure 8.19.: MB-ASM: Packet loss versus offered load for soft handover

express that the loss must not be smaller than zero.

$N_{\text{Lost,HO}}$ can be set to

$$N_{\text{Lost,HO}} = T_{\text{HO\_Lat}} r_{\text{Data}} \tag{8.21}$$

with the handover latency T_{HO_Lat} defined in Sect. 8.3.1 and the constant data rate r_{Data} in $\left(\frac{\text{packets}}{s}\right)$.

$N_{\text{Forw,HO}}$ is determined by two factors: The buffer size S_{Buff} and the age limit τ of the forwarding policy. The buffer size S_{Buff} in bytes bounds the maximum number of packets in the buffer to the queue length $l = \frac{S_{\text{Buff}}}{s_{\text{Pkt}}}$ where s_{Pkt} represents the constant packet size in bytes. The buffer is realized as a First In First Out (FIFO) queue. When a new packet arrives at the buffer with insufficient space left, the packet at the head of the queue is dropped and the new packet is stored at the tail of the queue. The age limit τ restricts the number of forwarded packets when the buffer is flushed – only those packets are forwarded that have a waiting time in the buffer smaller than τ. Otherwise a packet is not forwarded and dropped. Hence, the number of forwarded packets per handover $N_{\text{Forw,HO}}$ can be expressed by the number of packets that fill the buffer within the duration τ. If the number of packets exceeds the maximum number of packets in the buffer, then the number of forwarded packets is fixed by the buffer size. $N_{\text{Forw,HO}}$ can be expressed by the terms shown in Eq. (8.22).

$$N_{\text{Forw,HO}} = \begin{cases} \tau \; r_{\text{Data}} & \text{for } l > \tau \; r_{\text{Data}} \; , \\ l & \text{for } l \leq \tau \; r_{\text{Data}} \; . \end{cases} \tag{8.22}$$

Buffering and forwarding of packets are used for the predictive handover scheme only. Hence, for soft handover $N_{\text{Forw,HO}}$ equals 0. Consequently, for soft handover L_{HO} can be calculated by

$$L_{HO} = T_{\text{HO\_Lat}} \; r_{\text{Data}} \tag{8.23}$$

For predictive handover we come up with

$$L_{\mathrm{HO}} = \begin{cases} (T_{\mathrm{HO\_Lat}} - \tau)\ r_{\mathrm{Data}} & \text{for } T_{\mathrm{HO\_Lat}} \geq \tau \text{ and } l > \tau\ r_{\mathrm{Data}} \\ T_{\mathrm{HO\_Lat}}\ r_{\mathrm{Data}} - l & \text{for } T_{\mathrm{HO\_Lat}} < \frac{l}{r_{\mathrm{Data}}}\ \text{, and } l \leq \tau\ r_{\mathrm{Data}} \end{cases} \tag{8.24}$$

and

$$L_{\mathrm{HO}} = \begin{cases} 0 & \begin{array}{l} \text{for } T_{\mathrm{HO\_Lat}} < \tau \text{ and } l > \tau\ r_{\mathrm{Data}}\ , \\ \text{or} \\ \text{for } T_{\mathrm{HO\_Lat}} \geq \frac{l}{r_{\mathrm{Data}}}\ \text{, and } l \leq \tau\ r_{\mathrm{Data}}\ . \end{array} \end{cases} \tag{8.25}$$

The handover latency $T_{\mathrm{HO\_Lat}}$ in Eq. (8.24) and (8.25) can be expressed by the equations found in the previous section (listed in Tab. 8.9). Using the variable settings in Tab. 8.10 yield the theoretical results listed in Tab. 8.11.

Notation	Value
τ	5 s
S_{Buff}	100 kB
S_{Pkt}	1 kB

Table 8.10.: MB-ASM: Variable settings in the analytical evaluation of the packet loss and duplication

		Advertisement-based trigger	Link-layer trigger
Soft handover	LB	$0.105 * r_{\mathrm{Data}}$ pkts	$0.099 * r_{\mathrm{Data}}$ pkts
	UB	$0.345 * r_{\mathrm{Data}}$ pkts	$0.149 * r_{\mathrm{Data}}$ pkts
Predictive handover	LB	0	0
	UB	0	0

Table 8.11.: MB-ASM: Numerical results for the analysis of the packet loss

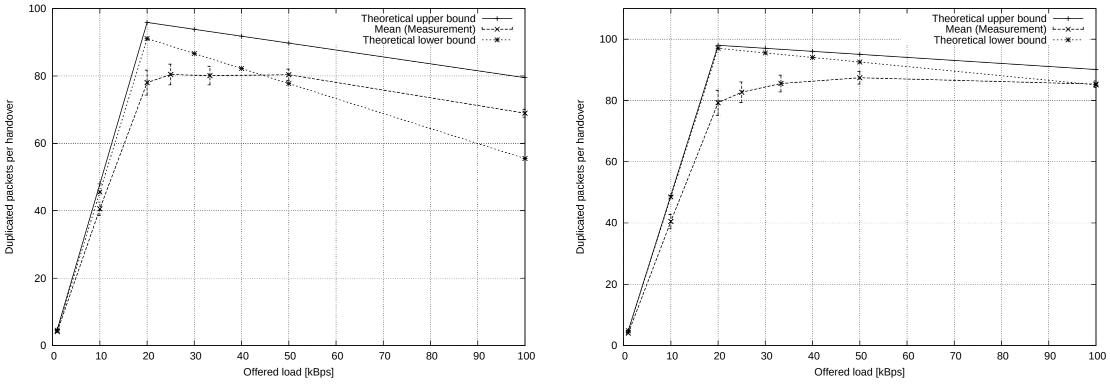
The packet duplication per handover D_{HO} can be easily derived from Eq. (8.20):

$$D_{HO} = \begin{cases} N_{\mathrm{Forw,HO}} - N_{\mathrm{Lost,HO}} & \text{for } N_{\mathrm{Forw,HO}} > N_{\mathrm{Lost,HO}}, \\ 0 & \text{else.} \end{cases} \tag{8.26}$$

Using Eq. (8.21) and Eq. (8.22) yields for soft handover

$$D_{\mathrm{HO}} = 0 \tag{8.27}$$

and for predictive handover



(a) Predictive handover, advertisement-based trigger

(b) Predictive handover, link-layer trigger

Figure 8.20.: MB-ASM: Packet duplication versus offered load for predictive handover

$$D_{\text{HO}} = \begin{cases} (\tau - T_{\text{HO\_Lat}})\ r_{\text{Data}} & \text{for } T_{\text{HO\_Lat}} < \tau \text{ and } l > \tau\ r_{\text{Data}}\ , \\ l - T_{\text{HO\_Lat}}\ r_{\text{Data}} & \text{for } T_{\text{HO\_Lat}} > \frac{l}{r_{\text{Data}}} \text{ and } l \leq \tau\ r_{\text{Data}}\ , \end{cases} \tag{8.28}$$

and

$$D_{\text{HO}} = \begin{cases} 0 & \begin{array}{l} \text{for } T_{\text{HO\_Lat}} \geq \tau \text{ and } l > \tau\ r_{\text{Data}}\ , \\ \text{or} \\ \text{for } T_{\text{HO\_Lat}} > \frac{l}{r_{\text{Data}}} \text{ and } l \leq \tau\ r_{\text{Data}}\ . \end{array} \end{cases} \tag{8.29}$$

The theoretical results for the packet duplication are summarized in Tab. 8.12. In Fig. 8.19 and 8.20 the 99 % confidence interval of the measured mean of L_{HO} and D_{HO} is between the lower and lower bound of the analysis.

		Advertisement-based trigger	**Link-layer trigger**
Soft	LB	0	0
handover	UB	0	0
Predictive	LB	$(4.795 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$	$(4.795 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$
handover		$(5 - 0.305 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$	$(5 - 0.305 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$
	UB	$(4.795 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$	$(4.795 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$
		$(5 - 0.305 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$	$(5 - 0.305 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$

Table 8.12.: MB-ASM: Numerical results for the analysis of the packet duplication

8.3.3. Relative TCP Throughput

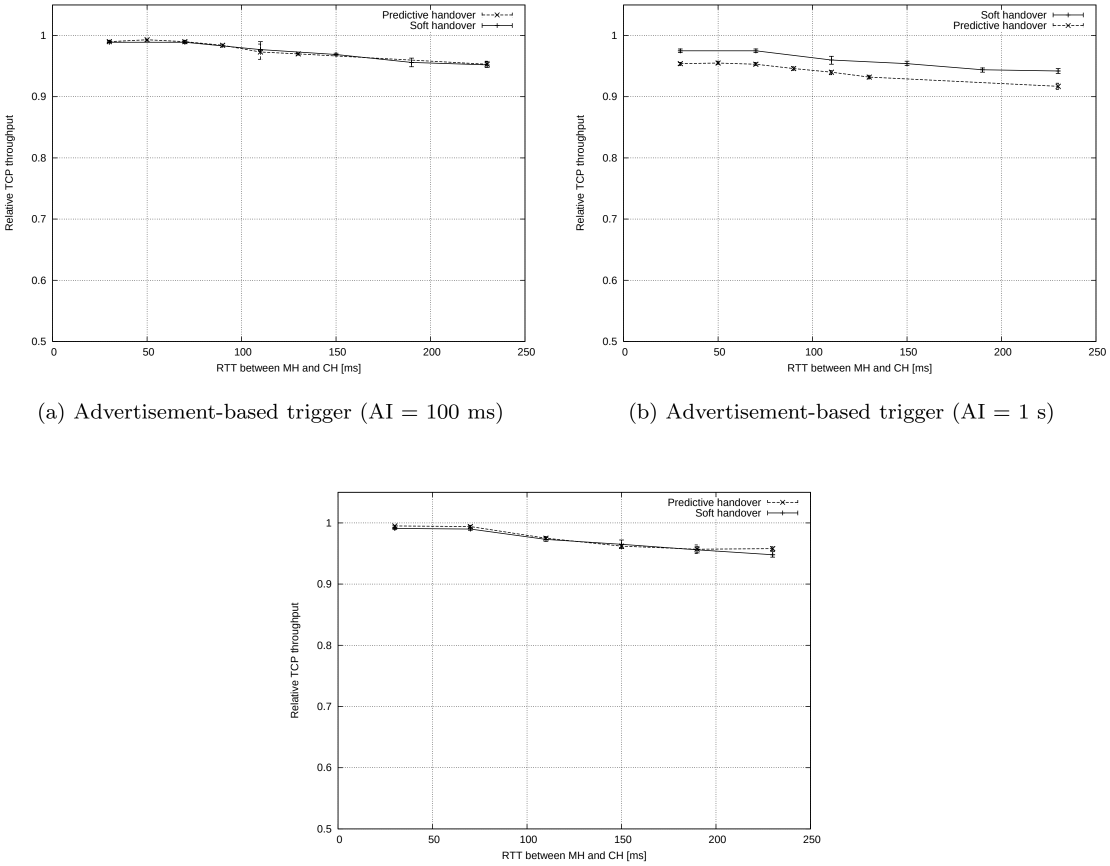
The relative TCP throughput B_{Rel} for a short-lived TCP connection with a single handover (Fig. 8.21) and for a long-lived TCP connection with multiple handovers (Fig. 8.22) is shown.

The experiments were conducted with the parameters in Tab. 8.6. The first experiment has examined a short-lived TCP connections with a duration of 60 s and a RTT varied from 30 ms to 230ms. The resulting relative TCP throughput is averaged over 100 values of the TCP throughput. In the second experiment a long-lived TCP connection was examined whereas the handover frequency was varied from 0 (no handover) to about 6 $\frac{\text{handover}}{\text{min}}$ by setting the *mean cell dwell time* parameter (Tab. 8.6). The RTT between the mobile host and the correspondent host was set to 130ms and remained constant. The duration of a measurement was adapted to the handover frequency: For rare handover events the duration of a measurement was increased, i.e. 9 hours for a handover frequency of 0.6 $\frac{\text{handover}}{\text{min}}$.

In Fig. 8.21 the relative throughput B_{Rel} of soft and predictive handover for a short-lived TCP connection with a single handover and an advertisement interval of 100 ms (Fig. 8.21(a)), 1 s (Fig. 8.21(b)), and link-layer trigger (Fig. 8.21(c)) is shown. B_{Rel} declines slightly with the RTT and is almost the same for soft and predictive handover, except for the case of an advertisement interval AI = 1 s, where the predictive handover shows a B_{Rel} reduced by a few percent.

In Fig. 8.22 the relative TCP throughput B_{Rel} of soft and predictive handover for a long-lived TCP connection and multiple handover with advertisement-based trigger and link-layer trigger is shown. For advertisement-based trigger with an advertisement interval of AI = 100 ms (Fig. 8.22(a)) and for link-layer trigger (Fig. 8.22(c)) B_{Rel} is almost the same: B_{Rel} decreases from 0.97 for 0.6 $\frac{\text{handover}}{\text{min}}$ to 0.85 for 6 $\frac{\text{handover}}{\text{min}}$. This can still be regarded as a moderate reduction of the TCP throughput. With AI = 1 s (Fig. 8.22(b)) B_{Rel} degrades: For 6 $\frac{\text{handover}}{\text{min}}$ the relative TCP throughput of the soft handover policy amounts to less than 30 % of the TCP throughput without handover. For predictive handover with an advertisement-based trigger of AI = 1 s (Fig. 8.22(b)) B_{Rel} degrades to 0.57. However, B_{Rel} is still significantly higher than for soft handover with the same advertisement interval ($B_{\mathrm{Rel}} \approx 0.29$).

It can be summarized, that for a high handover latency (e.g. caused by a long duration for handover detection, as in the case of AI = 1 s, and frequent handover the predictive handover scheme improves the relative TCP throughput. In the case of a short handover latency (as in the case of AI = 100 ms or link-layer trigger) the TCP throughput is not improved in comparison to soft handover.

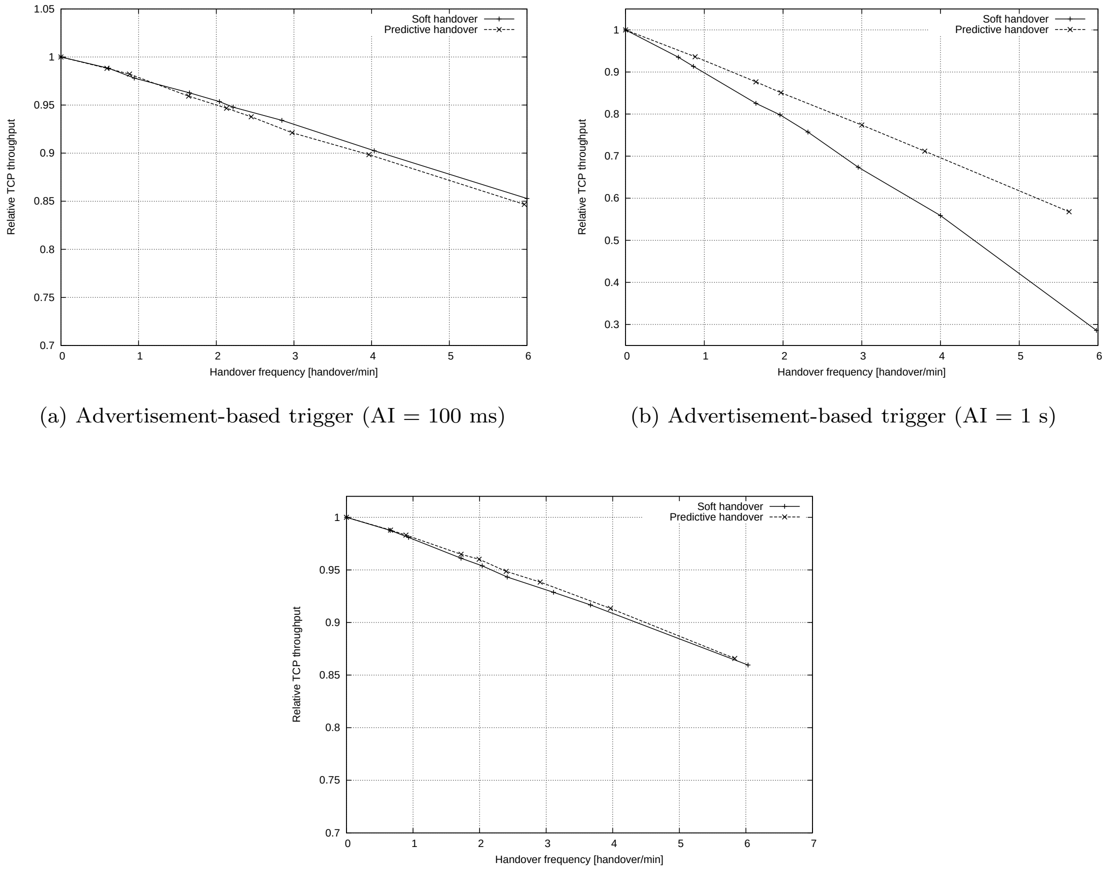


(a) Advertisement-based trigger (AI = 100 ms)

(b) Advertisement-based trigger (AI = 1 s)

(c) Link-layer trigger

Figure 8.21.: MB-ASM: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover



(a) Advertisement-based trigger (AI = 100 ms)

(b) Advertisement-based trigger (AI = 1 s)

(c) Link-layer trigger

Figure 8.22.: MB-ASM: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers

8.4. Performance Results for the Case Study MB-CMAP

In this section the handover performance results for the case study MB-CMAP are presented. As in the previous evaluation of the case study MB-ASM the results were gained by means of measurements and validated by analysis.

8.4.1. Handover Latency

In Fig. 8.23 the handover latency $T_{\text{HO\_Lat}}$ of hard, soft and predictive horizontal handover for advertisement-based trigger (Fig. 8.23(a), 8.23(c), and 8.23(e)) and link-layer trigger (Fig. 8.23(b), 8.23(d), and 8.23(f) is drawn.

The measurements were conducted with the same measurement procedure as for the case study MB-ASM, but with the testbed setup described in Sect. 8.1.2. Also, the parameters of the experiments were the same as listed in Tab. 8.6, except that in the case study MB-CMAP three handover policies were used (hard, soft, and predictive handover). Moreover, network address translation from IP unicast to IP multicast addresses was not necessary, and instead SAR were applied.

In Fig. 8.23(a) – 8.23(f) each point in the measurement graphs represents the mean value of the handover latency for about 230 handovers. As expected, the handover latency is independent of the round-trip time between the correspondent host and the mobile host. The mean handover latency of soft handover amounts to about 200 ms (link-layer trigger) and 500 ms (advertisement-based trigger). For predictive handover, the measured values are about 150 ms (link-layer trigger) and 500 ms (advertisement-based trigger).

In order to compare and validate the measurement results with theoretical values, the handover latency $T_{\text{HO\_Lat}}$ can be calculated with the same method used for the case study MB-ASM as described in Sect. 8.3.1. Since the latency to detect the handover $T_{\text{HO\_Detect}}$ is independent of the used multicast type, $T_{\text{HO\_Detect}}$ can be expressed by the same equations as for the case study MB-ASM for advertisement-based trigger (Eq. (8.11) and (8.12)) link-layer trigger (Eq. (8.13)), respectively. The handover latency of the execution $T_{\text{HO\_Exec}}$ of predictive handover can be written as

$$T_{\text{HO\_Exec, predictive}} = 2\ T_{\text{Proc,MH}} + T_{\text{RegReq}} + T_{\text{Proc,MEP}} + T_{\text{RegRepl}} \tag{8.30}$$

$T_{\text{HO\_Exec}}$ for hard and soft handover can be determined by Eq. (8.31).

$$T_{\text{HO\_Exec}} = 2T_{\text{Proc,MH}} + T_{\text{RegReq}} + T_{\text{Proc,MEP}} + T_{\text{CMAP\_MC}} + 2T_{\text{Pkt}} \tag{8.31}$$

In Eq. (8.31) $T_{\text{CMAP\_MC}}$ represents the duration of time needed for the execution of the particular CMAP multicast operations contributing to the handover latency. $T_{\text{CMAP\_MC}}$ for hard handover is given by Eq. (8.32)

$$T_{\text{CMAP\_MC, hard}} = T_{\text{Trace\_Call}} + T_{\text{Change\_Owner}} + T_{\text{Drop\_Ep}} + T_{\text{Add\_Ep}} \tag{8.32}$$

and for soft handover by Eq. (8.33)

$$T_{\text{CMAP\_MC, soft}} = T_{\text{Trace\_Call}} + T_{\text{Add\_Ep}} \tag{8.33}$$

The variables in Eq. (8.32) and (8.33) stand for the duration of time it takes to send and receive a CMAP *Trace_Call Request* and *Response* message ($T_{\text{Trace\_Call}}$), a CMAP *Change_Owner Request* and *Response* message ($T_{\text{Change\_Owner}}$), a CMAP *Drop_Ep Request* and *Response* message ($T_{\text{Drop\_Ep}}$), and a

Add_Ep Request and *Response* message ($T_{\text{Add\_Ep}}$), respectively. All variables include the processing in the switch controller and the invocation of other protocol entities in the switch controller.

Unlike in the case study MB-ASM it is not distinguished between lower and upper bounds for $T_{\text{HO\_Exec}}$ in the case study MB-CMAP. In MB-ASM the lower bound of $T_{\text{HO\_Exec}}$ is attained when the new access point is still subscribed for the mobile host's multicast group and the mobile host entry has not timed out yet. This situation cannot occur in the case study MB-CMAP since the old access point is actively dropped from the multicast distribution tree by the new access point. This functionality is termed *third party signalling* and is a feature of the CMAP/CMNP multicast protocol.

Again, it is assumed that

$$T_{\text{Proc,MH}} = T_{\text{Proc,MEP}} = \mathbf{T}_{\text{Proc}} \tag{8.34}$$

and

$$T_{\text{Advert}} = T_{\text{Solicit}} = T_{\text{RegReq}} = T_{\text{RegRepl}} = T_{\text{Pkt}} = \mathbf{T}_{\text{Msg}} \tag{8.35}$$

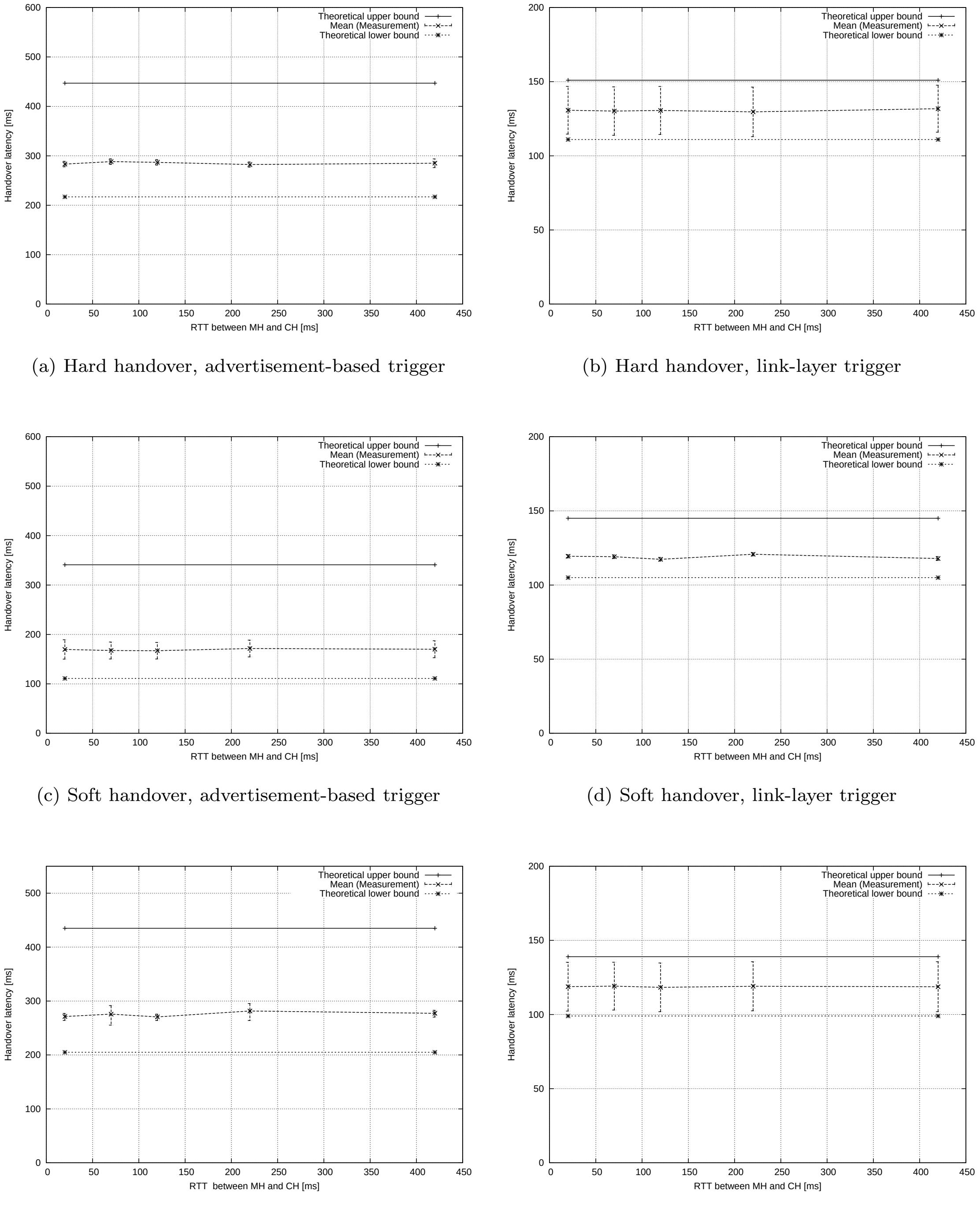
It is noted that the CMAP-specific operations cannot be replaced by T_{Proc} as in Eq.(8.34) since their processing time is expected to be much higher.

The equations for the calculation of the handover latency $T_{\text{HO\_Lat}}$ are summarized in Tab. 8.13. The variables are set to the values listed in Tab. 8.14. It is noted that the CMAP operations *Change_Owner*, *Drop_Ep*, and *Add_Ep* incorporate actions of underlying protocol entities belonging to the CMAP protocol stack, such as CMNP and NCCP. The duration of time needed for these actions, including the inter-process communication, contribute directly to the overall duration needed for the CMAP operations. The variable settings for the CMAP operations are typical values based on measurements. Details of these measurement results can be found in [14]. The numerical results for the analysis of the handover latency as listed in Tab. 8.15.

		Advertisement-based trigger	**Link-layer trigger**
Hard handover	LB	$3T_{\text{Proc}} + 3T_{\text{Msg}} + \frac{2}{r_{\text{Advert}}} + T_{\text{Trace\_Call}} + T_{\text{Change\_Owner}} + T_{\text{Drop\_Ep}} + T_{\text{Add\_Ep}}$	$5T_{\text{Proc}} + 5T_{\text{Msg}} + T_{\text{Mov}} + T_{\text{Trace\_Call}} + T_{\text{Change\_Owner}} + T_{\text{Drop\_Ep}} + T_{\text{Add\_Ep}}$
	UB	$3T_{\text{Proc}} + 3T_{\text{Msg}} + T_{\text{Mov}} + \frac{3}{r_{\text{Advert}}} + T_{\text{Trace\_Call}} + T_{\text{Change\_Owner}} + T_{\text{Drop\_Ep}} + T_{\text{Add\_Ep}}$	$5T_{\text{Proc}} + 5T_{\text{Msg}} + T_{\text{Mov}} + T_{\text{Trace\_Call}} + T_{\text{Change\_Owner}} + T_{\text{Drop\_Ep}} + T_{\text{Add\_Ep}}$
Soft handover	LB	$3T_{\text{Proc}} + 3T_{\text{Msg}} + \frac{1}{r_{\text{Advert}}} + T_{\text{Trace\_Call}} + T_{\text{Add\_Ep}}$	$5T_{\text{Proc}} + 5T_{\text{Msg}} + T_{\text{Mov}} + T_{\text{Trace\_Call}} + T_{\text{Add\_Ep}}$
	UB	$3T_{\text{Proc}} + 3T_{\text{Msg}} + T_{\text{Mov}} + \frac{2}{r_{\text{Advert}}} + T_{\text{Trace\_Call}} + T_{\text{Add\_Ep}}$	$5T_{\text{Proc}} + 5T_{\text{Msg}} + T_{\text{Mov}} + T_{\text{Trace\_Call}} + T_{\text{Add\_Ep}}$
Predictive handover	LB	$3T_{\text{Proc}} + 2T_{\text{Msg}} + \frac{2}{r_{\text{Advert}}}$	$5T_{\text{Proc}} + 4T_{\text{Msg}} + T_{\text{Mov}}$
	UB	$3T_{\text{Proc}} + 2T_{\text{Msg}} + T_{\text{Mov}} + \frac{3}{r_{\text{Advert}}}$	$5T_{\text{Proc}} + 4T_{\text{Msg}} + T_{\text{Mov}}$

Table 8.13.: MB-CMAP: Analytical results of the handover latency

Fig. 8.24 compares the handover latency for vertical and horizontal handover (mean with 99 % confidence interval). Similar to the vertical handover in MB-ASM (Sect. 8.3.1) the mean handover



(a) Hard handover, advertisement-based trigger

(b) Hard handover, link-layer trigger

(c) Soft handover, advertisement-based trigger

(d) Soft handover, link-layer trigger

(e) Predictive handover, advertisement-based trigger

(f) Predictive handover, link-layer trigger

Figure 8.23.: MB-CMAP: Handover latency versus RTT between CH and MH

Variable	**Value**
r_{Advert}	$\frac{10}{s}$
T_{Add_Ep}, T_{Drop_Ep}, T_{Change_Owner}	3 ms
T_{Mov}	90 – 130 ms
T_{Msg}	1 ms
T_{Trace_Call}, T_{Trace_Ep}	2 ms
T_{Proc}	1 ms

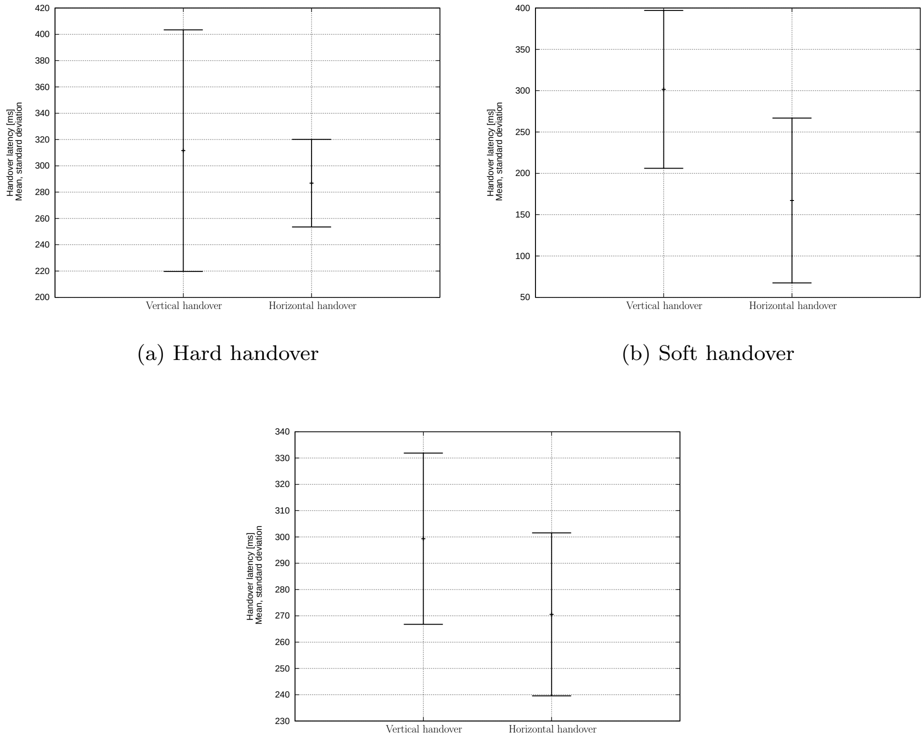
Table 8.14.: MB-CMAP: Variable settings in the analytical evaluation of the handover latency

		Advertisement-based trigger	**Link-layer trigger**
Hard handover	LB	217 ms	111 ms
	UB	447 ms	151 ms
Soft handover	LB	111 ms	105 ms
	UB	341 ms	145 ms
Predictive handover	LB	205 ms	99 ms
	UB	435 ms	139 ms

Table 8.15.: MB-CMAP: Numerical results for the analysis of the handover latency

latency for vertical handover is higher than for horizontal handover. Again, this is caused by the different method to trigger the handover in the experimental setup: The additional latency for vertical handover corresponds approximately with the duration to switch on/off the additional ports for the vertical handover.

In Fig. 8.23 the 99% confidence intervals of the mean handover latency $T_{\mathrm{HO\_Lat}}$ is between the theoretical lower and upper bound attained from analysis.



(a) Hard handover

(b) Soft handover

(c) Predictive handover

Figure 8.24.: MB-CMAP: Comparison of the handover latency versus RTT between CH and MH for vertical and horizontal handover

8.4.2. Packet Loss and Duplication

In Fig. 8.25 the packet loss L_{HO} and the packet duplication D_{HO} of hard, soft, and predictive handover for advertisement-based trigger and link-layer trigger are plotted. The figures include the results from the measurements and the analysis.

For the experiments the same measurement procedure as in the case study MB-ASM was applied. For hard and soft handover with advertisement-based trigger the measurement graphs of L_{HO} in Fig. 8.25 show a linear growing L_{HO} up to about 26 packets (hard handover) and 14 packets (soft handover) for an offered load of 100 kBps. For link-layer trigger L_{HO} amounts to 11 packets at the same offered load. For hard and soft handover no packet duplication was observed ($D_{HO} = 0$).

For predictive handover L_{HO} is 0 for both, advertisement-based and link-layer trigger. As seen in Fig. 8.25 D_{HO} linearly grows up to a maximum of about 90 packets at a load of 20 kBps and decreases slightly at higher loads.

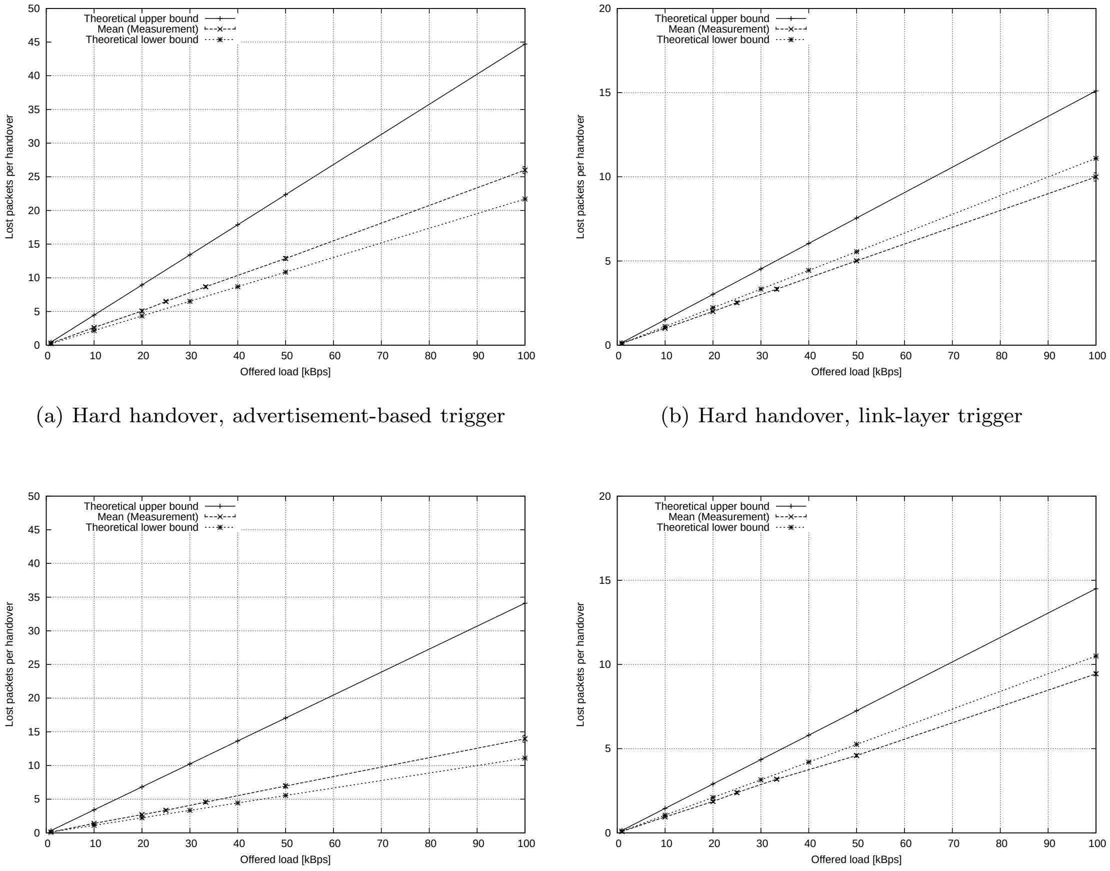
For the analysis of the packet loss and packet duplication, the equations derived in the case study MB-ASM (Eq. (8.20) – (8.29)) can be used. The results are listed in Tab. 8.16 and 8.17.

		Advertisement-based trigger	**Link-layer trigger**
Hard handover	LB	$0.217 * r_{\text{Data}}$ pkts	$0.111 * r_{\text{Data}}$ pkts
	UB	$0.447 * r_{\text{Data}}$ pkts	$0.151 * r_{\text{Data}}$ pkts
Soft handover	LB	$0.111 * r_{\text{Data}}$ pkts	$0.105 * r_{\text{Data}}$ pkts
	UB	$0.341 * r_{\text{Data}}$ pkts	$0.145 * r_{\text{Data}}$ pkts
Predictive handover	LB	0	0
	UB	0	0

Table 8.16.: MB-CMAP: Numerical results for the analysis of the packet loss

		Advertisement-based trigger	**Link-layer trigger**
Hard handover	LB	0	0
	UB	0	0
Soft handover	LB	0	0
	UB	0	0
Predictive handover	LB	$(4.795 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$ $(5 - 0.205 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$	$(4.901 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$ $(5 - 0.099 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$
	UB	$(4.565 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$ $(5 - 0.435 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$	$(4.861 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} < 20)$ $(5 - 0.139 * r_{\text{Data}})$ pkts for $(r_{\text{Data}} \geq 20)$

Table 8.17.: MB-CMAP: Numerical results for the analysis of the packet duplication



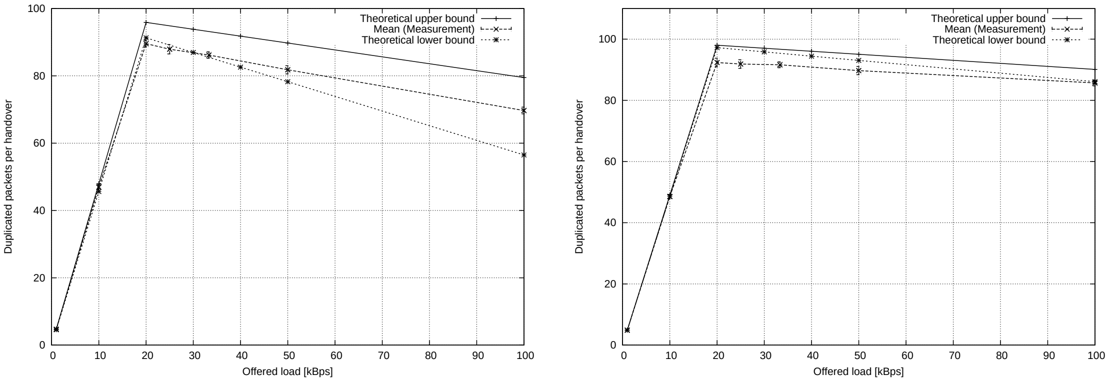
(a) Hard handover, advertisement-based trigger

(b) Hard handover, link-layer trigger

(c) Soft handover, advertisement-based trigger

(d) Soft handover, link-layer trigger

Figure 8.25.: MB-CMAP: Packet loss versus offered load for soft handover



(a) Predictive handover, advertisement-based trigger

(b) Predictive handover, link-layer trigger

Figure 8.26.: MB-CMAP: Packet duplication versus offered load for predictive handover

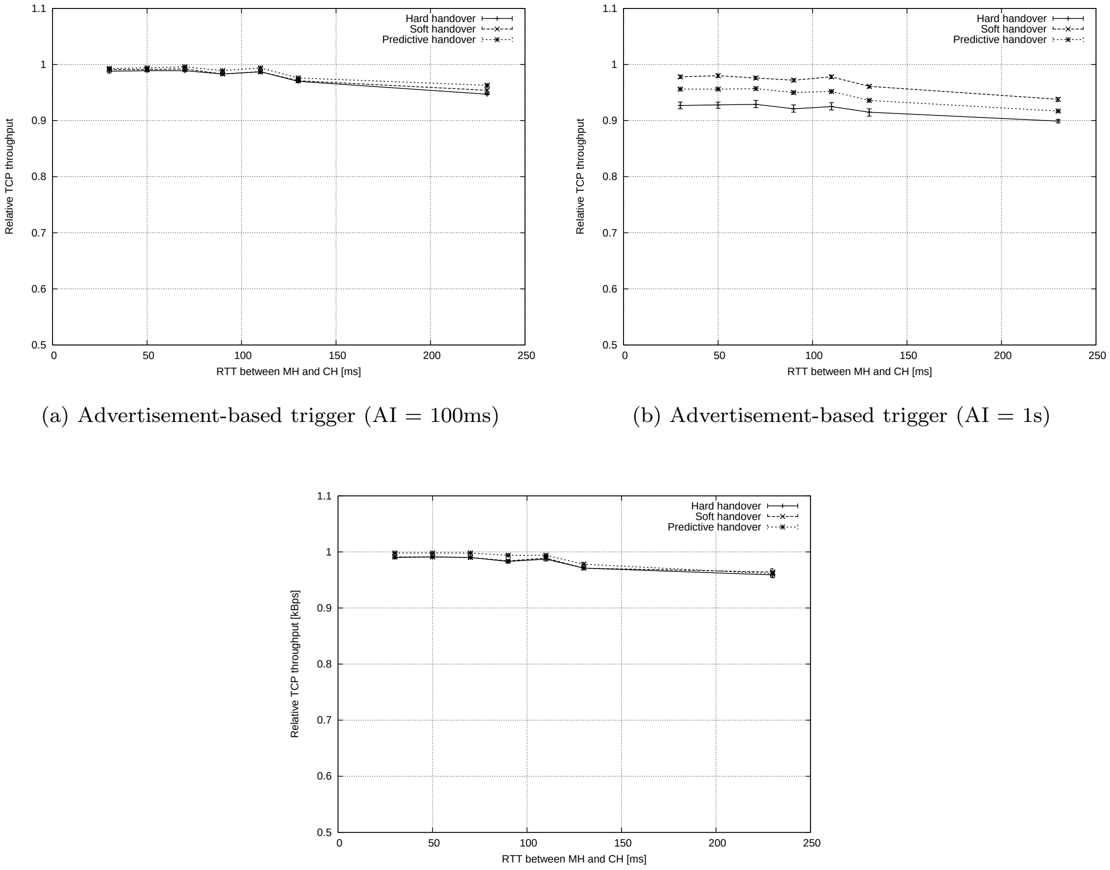
8.4.3. Relative TCP Throughput

The relative TCP throughput B_{Rel} of a short-lived TCP connection with a single handover and for a long-lived TCP connection with multiple handover for advertisement-based trigger and link-layer trigger is shown in Fig. 8.27 and Fig. 8.28, respectively. The parameters are the same as described for the case study MB-ASM (Sect. 8.3.3).

The experiments with a short-lived TCP connection and a single handover show a very similar behavior for advertisement-based handover with an advertisement-interval of 100ms and link-layer trigger for hard, soft, and predictive handover in Fig. 8.27(a) and Fig. 8.27(c): B_{Rel} decreases slightly to about 95 %. For advertisement-based trigger with an advertisement interval of AI = 1 s the soft handover has a better performance than predictive (93 %) and hard handover (90 %).

For a long-lived TCP connection with multiple handover the measurement graphs show a very similar B_{Rel} for hard and soft handover: For both advertisement-based trigger (AI = 100 ms, Fig. 8.28(a)) and link-layer trigger (Fig. 8.28(c)) B_{Rel} decreases linearly to $B_{\mathrm{Rel}} \approx 0.83$ at about $6 \frac{\mathrm{handover}}{\mathrm{min}}$.

With an advertisement-based trigger of AI = 1 s (Fig. 8.28(b)) B_{Rel} degrades: B_{Rel} of the hard handover policy is reduced to ≈ 0.45 at a handover frequency of $6 \frac{\mathrm{handover}}{\mathrm{min}}$. The predictive handover scheme improves B_{Rel} of hard handover considerably (0.62 at 6 $\frac{\mathrm{handover}}{\mathrm{min}}$), but the soft handover policy achieves a relative TCP throughput of 0.77.

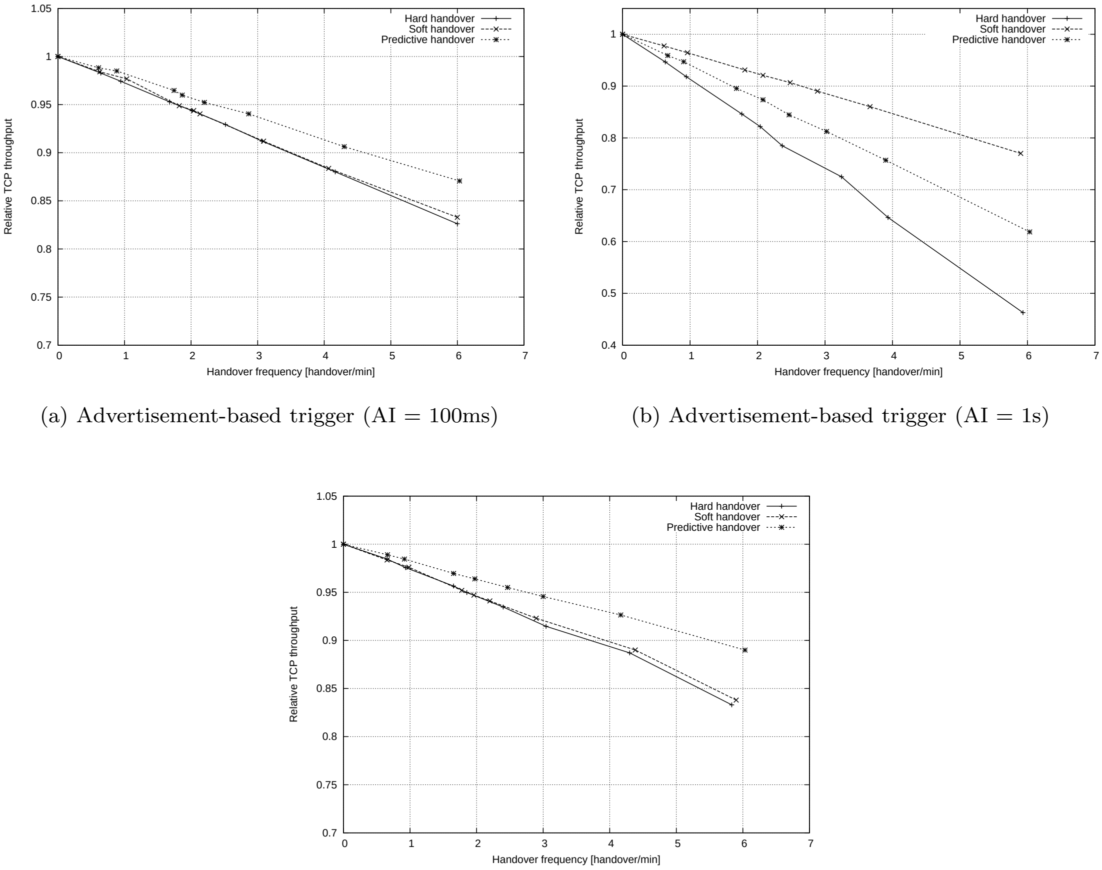


(a) Advertisement-based trigger (AI = 100ms)

(b) Advertisement-based trigger (AI = 1s)

(c) Link-layer trigger

Figure 8.27.: MB-CMAP: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover



(a) Advertisement-based trigger (AI = 100ms)

(b) Advertisement-based trigger (AI = 1s)

(c) Link-layer trigger

Figure 8.28.: MB-CMAP: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers

8.5. Performance Results for the Case Study MIP-SGM

In this section the handover performance results for the case study MIP-SGM are presented. A subset of the simulation model was verified by comparing the simulation results with measurement results of basic Mobile IP and hierarchical Mobile IP (see Appendix B). In addition, the simulation results are validated by means of analysis.

8.5.1. Handover Latency

In Fig. 8.29 the handover latency $T_{\mathrm{HO\_Lat}}$ of soft handover for advertisement-based trigger (Fig. 8.29(a) and 8.29(c)) and for link-layer trigger (Fig. 8.29(b) and 8.29(d)) is shown.

The results are gained by experiments in the simulation setup described in Sect. 8.1.3. It is worth noting that in the simulation setup a model of a wireless LAN (IEEE 02.11) is used whereas in the measurement setup for basic and hierarchical Mobile IP the wireless links were replaced by Ethernet. Tab. 8.18 lists the simulation parameters. In order to have a comparable evaluation environment for simulation and measurements a *cell gap* parameter Tab. 8.18 is introduced. This parameter considers the duration of time that is introduced by the method to trigger a handover in the measurement setup, where a handover is triggered by means of SNMP-controlled switching of Ethernet ports in a hub.

Notation	**Value**
Traffic type	UDP
Direction of traffic flow	Downlink
Packet size [Bytes]	1024
Packet burst size [N]	1
Inter burst time [ms]	10
Mean value of exponential CDT distribution [s]	10
Offset ϵ [s]	5
Cell gap [ms]	100 ms (Non-overlapping cells)
WAN delay [ms]	0, 10,20,30,40,50,100
FA Advertisement interval [s]	0.1
FA Advertisement lifetime [s]	0.3
Re-registration interval [s]	10
Registration lifetime [s]	30
Handover initiation policy	Advertisement-based trigger
Handover type	Horizontal, vertical
Tunnel lifetime [s]	600s
Tunneling type	Reverse tunneling
Foreign agent packet capsulation	Enabled (No co-located FA)
Test length [min]	60

Table 8.18.: MIP-SGM: Simulation parameters

The simulation results are validated by analysis as follows: Using advertisement-based handover trigger, the mobile host sends a simultaneous binding when it receives an advertisement from a new foreign agent. In contrast, in basic and hierarchical Mobile IP a registration is sent when the advertisement lifetime of the old foreign agent expires. Hence, for advertisement-based trigger $T_{\text{HO\_Detect}}$ is given by

$$T_{\text{HO\_Detect, lower bound}} = T_{\text{Mov}} \tag{8.36}$$

$$T_{\text{HO\_Detect, upper bound}} = T_{\text{Mov}} + \frac{1}{r_{\text{Advert}}} + T_{\text{Advert\_Defer,Max}} \tag{8.37}$$

with the following variables:

T_{Mov} Duration of mobile host's physical movement from one wireless to another in the case of non-overlapping cells [ms],

r_{Advert} Advertisement rate $\left[\frac{1}{s}\right]$,

$T_{Advert\_Defer,Max}$ Maximum duration of advertisement deferral.

For link-layer trigger $T_{\text{HO\_Detect}}$ is

$$\begin{aligned} T_{\text{HO\_Detect, lower bound}} &= T_{\text{HO\_Detect, upper bound}} && (8.38)\\ &= T_{\text{Mov}} + T_{\text{Proc,MH}} + T_{\text{Solicit}} + T_{\text{Proc,MEP}} + T_{\text{Advert}} && (8.39) \end{aligned}$$

$T_{\text{HO\_Exec}}$ for SGM-enhanced basic Mobile IP can be expressed by

$$\begin{aligned} T_{\text{HO\_Exec}} = {} & 2T_{\text{Proc,MH}} + T_{\text{RegReq,MH} \rightarrow \text{FA}} + T_{\text{Proc,FA}} + T_{\text{RegReq,FA} \rightarrow \text{HA}} \\ & + T_{\text{Proc,HA}} + T_{\text{RegRepl,HA} \rightarrow \text{FA}} + T_{\text{Proc,FA}} + T_{\text{RegRepl,FA} \rightarrow \text{MH}} \end{aligned} \tag{8.40}$$

and for SGM-enhanced hierarchical Mobile IP

$$\begin{aligned} T_{\text{HO\_Exec}} = {} & 2T_{\text{Proc,MH}} + T_{\text{RegReq,MH} \rightarrow \text{LFA}} + T_{\text{Proc,LFA}} + T_{\text{RegReq,LFA} \rightarrow \text{HFA}} \\ & + T_{\text{Proc,HFA}} + T_{\text{RegRepl,HFA} \rightarrow \text{LFA}} + T_{\text{Proc,LFA}} + T_{\text{RegRepl,LFA} \rightarrow \text{MH}} \end{aligned} \tag{8.41}$$

with

$T_{Proc,\mathbf{Node}}$ Duration of message processing in a *node*, where MH stands for mobile, host, FA for foreign agent, LFA and HFA for lowest and highest foreign agent, respectively, and HA for home agent,

$T_{RegReq,\mathbf{Node\ A} \rightarrow \mathbf{Node\ B}}$ Duration for the transmission of a *Registration Request* message from *Node A* to *Node B*, where *Node A* or *Node B* can be FA (Foreign Agent), LFA (Lowest Foreign Agent), HFA (Highest Foreign Agent), and HA (Home Agent),

$T_{RegRepl,\mathbf{Node\ A} \rightarrow \mathbf{Node\ B}}$ Duration for the transmission of a *Registration Reply* message from *Node A* to *Node B*, with the same meaning for *Node A* and *Node B* as above,

$T_{RegRepl,\mathbf{Node\ A} \rightarrow \mathbf{Node\ B}}$ Duration for the transmission of a *Registration Reply* message from *Node A* to *Node B*, where *Node A* and *Node B* stand for HA, FA, LFA, HFA, and HA, respectively.

Similar to the previous analysis it is assumed that

$$\mathbf{T}_{\text{Proc}} = T_{\text{Proc,MH}} = T_{\text{Proc,FA}} = T_{\text{Proc,LFA}} = T_{\text{Proc,HFA}} = T_{\text{Proc,HA}} \tag{8.42}$$

and

$$\begin{aligned} \mathbf{T}_{\text{Msg}} &= T_{\text{Advert}} = T_{\text{Solicit}} \\ &= T_{\text{RegReq,MH} \rightarrow \text{FA}} = T_{\text{RegRepl,FA} \rightarrow \text{MH}} \qquad (8.43) \\ &= T_{\text{RegReq,MH} \rightarrow \text{LFA}} = T_{\text{RegRepl,LFA} \rightarrow \text{MH}} \\ &= T_{\text{RegRepl,HFA} \rightarrow \text{LFA}} = T_{\text{RegReq,LFA} \rightarrow \text{HFA}} \qquad (8.44) \end{aligned}$$

Eq. (8.43) does not include $T_{\text{RegRepl,FA} \rightarrow \text{HA}}$ and $T_{\text{RegRepl,HA} \rightarrow \text{FA}}$. However, both terms can be equated:

$$T_{\text{RegReq,FA} \rightarrow \text{HA}} = T_{\text{RegRepl,HA} \rightarrow \text{FA}} \tag{8.45}$$

The equations for the overall handover latency $T_{\text{HO\_Lat}}$ are summarized in Tab. 8.19.

		Advertisement-based trigger	**Link-layer trigger**
Basic MIP-SGM	LB	$5T_{\text{Proc}}+2T_{\text{Msg}}+2T_{\text{RegReq,FA} \rightarrow \text{HA}}+T_{\text{Mov}}$	$T_{\text{Mov}}+7T_{\text{Proc}}+4T_{\text{Msg}}+2T_{\text{RegReq,FA} \rightarrow \text{HA}}$
	UB	$5T_{\text{Proc}} + 2T_{\text{Msg}} + 2T_{\text{RegReq,FA} \rightarrow \text{HA}} + T_{\text{Mov}} + T_{\text{Advert\_Defer,Max}} + \frac{1}{r_{\text{Advert}}}$	$T_{\text{Mov}} + 7T_{\text{Proc}} + 4T_{\text{Msg}} + 2T_{\text{RegReq,FA} \rightarrow \text{HA}} + T_{\text{Advert\_Defer,Max}}$
Hierarchical MIP-SGM	LB	$7T_{\text{Proc}} + 6T_{\text{Msg}} + T_{\text{Mov}}$	$T_{\text{Mov}} + 7T_{\text{Proc}} + 6T_{\text{Msg}}$
	UB	$5T_{\text{Proc}}+4T_{\text{Msg}}+T_{\text{Mov}}+T_{\text{Advert\_Defer,Max}}+\frac{1}{r_{\text{Advert}}}$	$T_{\text{Mov}} + 7T_{\text{Proc}} + 6T_{\text{Msg}} + T_{\text{Advert\_Defer,Max}}$

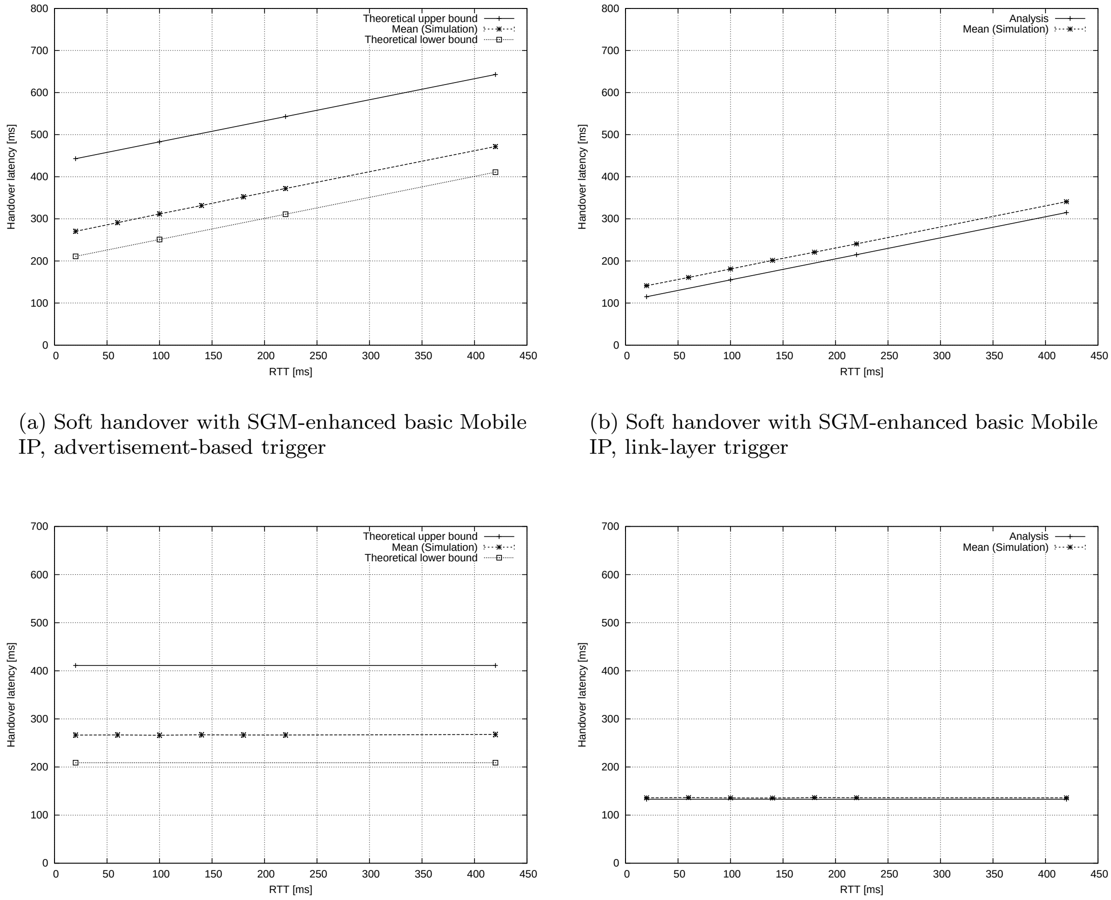
Table 8.19.: MIP-SGM: Analytical results of the handover latency

Notation	**Value**
T_{Msg}	1 ms
r_{Advert}	$\frac{10}{s}$
T_{Proc}	1 ms
$T_{RegReq,FA \rightarrow HA}$	2 ms, 22 ms, 52 ms, 102 ms
T_{Mov}	100 ms
$T_{Advert\_Defer,Max}$	2 ms

Table 8.20.: MIP-SGM: Variable settings in the analytical evaluation of the handover latency

		Advertisement-based trigger	**link-layer trigger**
Basic	LB	107 ms + $2T_{\text{RegReq,FA} \rightarrow \text{HA}}$	111 ms + $2T_{\text{RegReq,FA} \rightarrow \text{HA}}$
MIP-SGM	UB	209 ms + $2T_{\text{RegReq,FA} \rightarrow \text{HA}}$	113 ms + $2T_{\text{RegReq,FA} \rightarrow \text{HA}}$
Hierarchical	LB	109 ms	113 ms
MIP-SGM	UB	211 ms	115 ms

Table 8.21.: MIP-SGM: Numerical results for the analysis of the handover latency



(a) Soft handover with SGM-enhanced basic Mobile IP, advertisement-based trigger

(b) Soft handover with SGM-enhanced basic Mobile IP, link-layer trigger

(c) Soft handover with SGM-enhanced hierarchical Mobile IP, advertisement-based trigger

(d) Soft handover with SGM-enhanced hierarchical Mobile IP, link-layer trigger

Figure 8.29.: MIP-SGM: Handover latency versus RTT between CH and MH

8.5.2. Packet Loss and Duplication

In Fig. 8.30 the packet loss L_{HO} of basic and hierarchical MIP-SGM for advertisement-based trigger (Fig. 8.30(a) and 8.30(c)) and link-layer trigger (Fig. 8.30(b) and 8.30(d)) is shown. The figures include the results from the simulation and the analysis. The same simulation parameter as in Tab. 8.18 were used, except that the offered load was varied from 1 kBps to 100 kBps by modifying the inter-packet time at a constant packet size of 1 kBps. The RTT between the mobile host and the correspondent host was set to about 120 ms.

For MIP-SGM with basic Mobile IP the measurement graph of L_{HO} in Fig. 8.30(a) grows linearly up to 22 packets per handover for an offered load of 100 kBps. For link-layer trigger L_{HO} amounts to about 20 packets at an offered load of 100 kBps. For MIP-SGM based on hierarchical Mobile IP (Fig. 8.11(b) and 8.30(d)) the packet loss increases to about 17 packets for advertisement-based trigger and to about 12 packets for link-layer trigger at the same offered load. In all simulated scenarios no duplicated packets were observed ($D_{HO} = 0$).

The theoretical packet loss for a constant data rate can simply be calculated by Eq. (8.46). Using the numerical results for the handover latency $T_{\text{HO\_Lat}}$ calculated in Sect. 8.2.1 gives the theoretical results for L_{HO} listed in Tab. 8.22.

$$L_{HO} = N_{\text{Lost,HO}} = T_{\text{HO\_Lat}} r_{\text{Data}} \tag{8.46}$$

		Advertisement-based trigger	**Link-layer trigger**
Basic	LB	$(0.107 + 2T_{\text{RegReq,FA} \rightarrow \text{HA}}) * r_{\text{Data}}$ pkts	$(0.111 + 2T_{\text{RegReq,FA} \rightarrow \text{HA}}) * r_{\text{Data}}$ pkts
MIP-SGM	UB	$(0.209 + 2T_{\text{RegReq,FA} \rightarrow \text{HA}}) * r_{\text{Data}}$ pkts	$(0.113 + 2T_{\text{RegReq,FA} \rightarrow \text{HA}}) * r_{\text{Data}}$ pkts
Hierarchical	LB	$0.109 * r_{\text{Data}}$ pkts	$0.113 * r_{\text{Data}}$ pkts
MIP-SGM	UB	$0.211 * r_{\text{Data}}$ pkts	$0.115 * r_{\text{Data}}$ pkts

Table 8.22.: MIP-SGM: Numerical results for the analysis of the packet loss

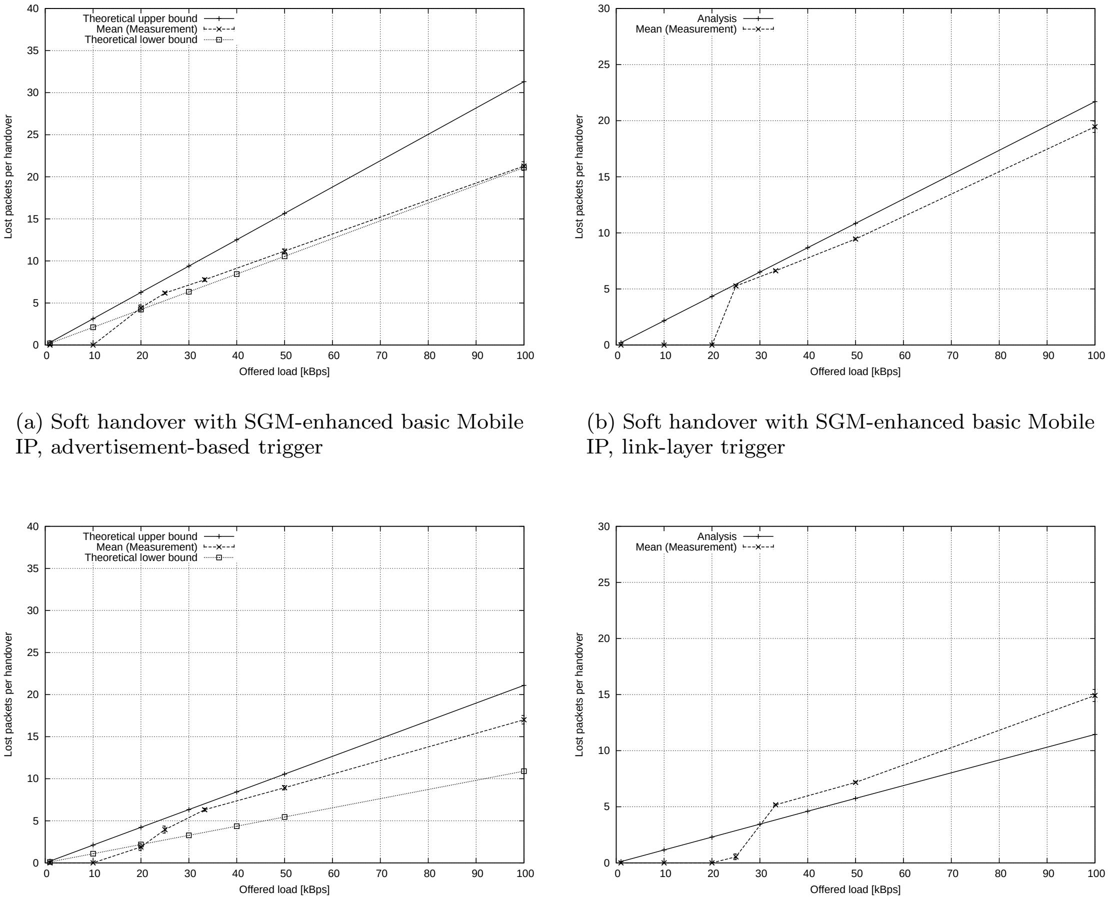
8.5.3. Relative TCP Throughput

The relative TCP throughput B_{Rel} of basic and hierarchical MIP-SGM for a short-lived TCP connection with a single handover and a long-lived TCP connection with multiple handovers is shown in Fig. 8.31 and 8.32, respectively.

The parameters are the same as described for the case study MB-ASM and MB-CMAP (Sect. 8.3.3) and 8.4.3).

Regarding the experiments with a short-lived TCP connection and a single handover, B_{Rel} is reduced moderately to about 0.9 for SGM-enhanced basic and hierarchical Mobile IP for advertisement-based trigger (Fig. 8.31(a) and 8.31(c)) and link-layer trigger (Fig. 8.31(b) and 8.31(d)), whereas B_{Rel} for SGM-enhanced basic Mobile IP is slightly better than for SGM-enhanced hierarchical Mobile IP.

Regarding the experiments with a long-lived TCP connection and multiple handover, B_{Rel} is reduced to about 0.9 at a handover frequency of $6\,\frac{\text{handover}}{\text{min}}$ for SGM-enhanced basic and hierarchical Mobile IP for advertisement-based trigger (advertisement interval 100 ms) and link-layer trigger. For an advertisement interval of 1 s the B_{Rel} degrades to about 0.67 for SGM-enhanced basic Mobile IP and 0.62 for SGM-enhanced hierarchical Mobile IP at a handover frequency of $6\,\frac{\text{handover}}{\text{min}}$.



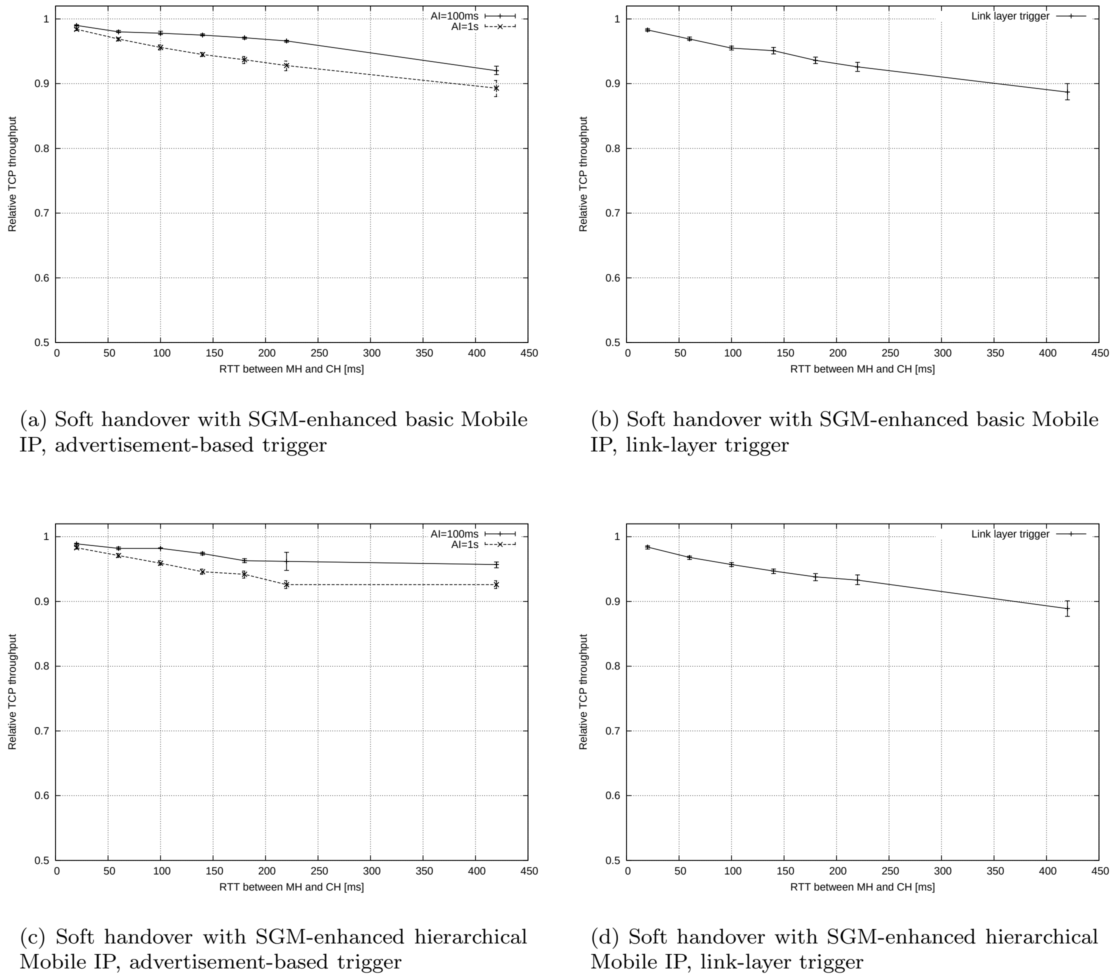
(a) Soft handover with SGM-enhanced basic Mobile IP, advertisement-based trigger

(b) Soft handover with SGM-enhanced basic Mobile IP, link-layer trigger

(c) Soft handover with SGM-enhanced hierarchical Mobile IP, advertisement-based trigger

(d) Soft handover with SGM-enhanced hierarchical Mobile IP, link-layer trigger

Figure 8.30.: MIP-SGM: Packet loss versus offered load



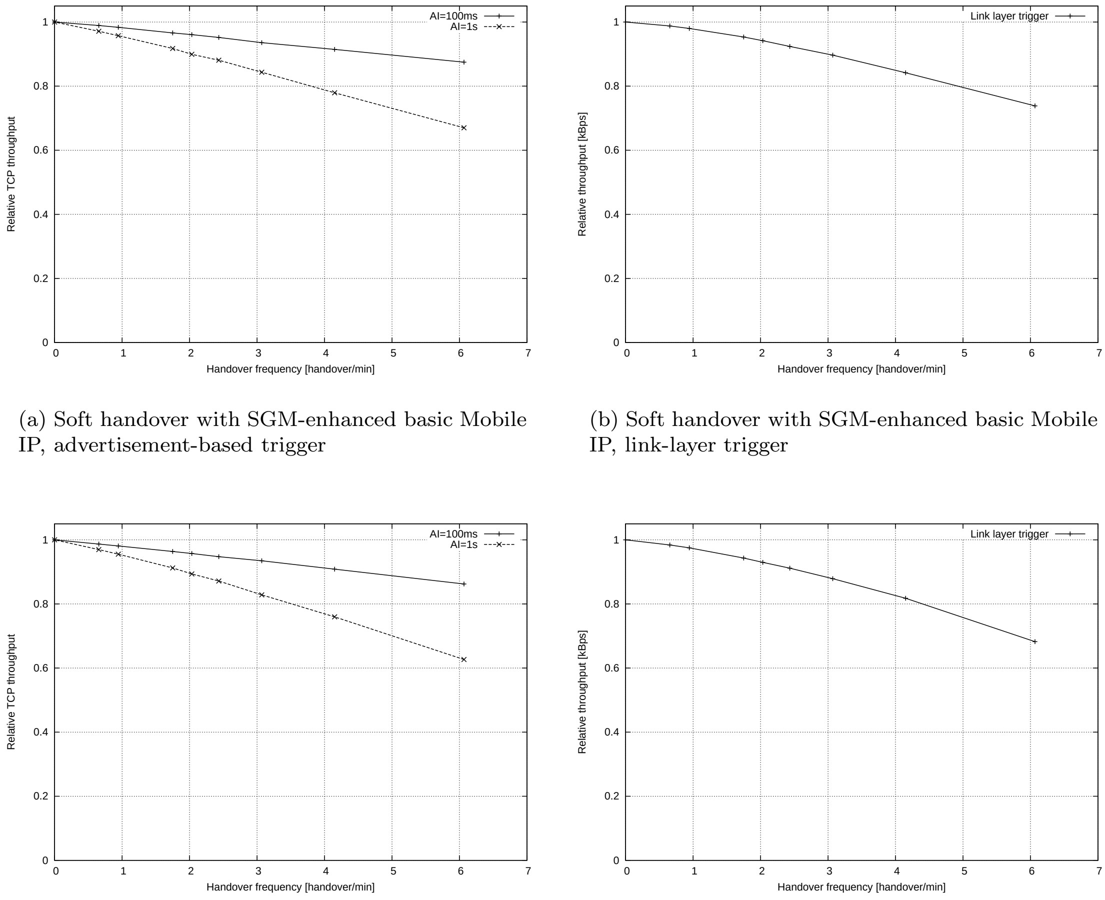
(a) Soft handover with SGM-enhanced basic Mobile IP, advertisement-based trigger

(b) Soft handover with SGM-enhanced basic Mobile IP, link-layer trigger

(c) Soft handover with SGM-enhanced hierarchical Mobile IP, advertisement-based trigger

(d) Soft handover with SGM-enhanced hierarchical Mobile IP, link-layer trigger

Figure 8.31.: MIP-SGM: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover



(a) Soft handover with SGM-enhanced basic Mobile IP, advertisement-based trigger

(b) Soft handover with SGM-enhanced basic Mobile IP, link-layer trigger

(c) Soft handover with SGM-enhanced hierarchical Mobile IP, advertisement-based trigger

(d) Soft handover with SGM-enhanced hierarchical Mobile IP, link-layer trigger

Figure 8.32.: MIP-SGM: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers

8.6. Performance Comparison of the Case Studies and the Reference Case

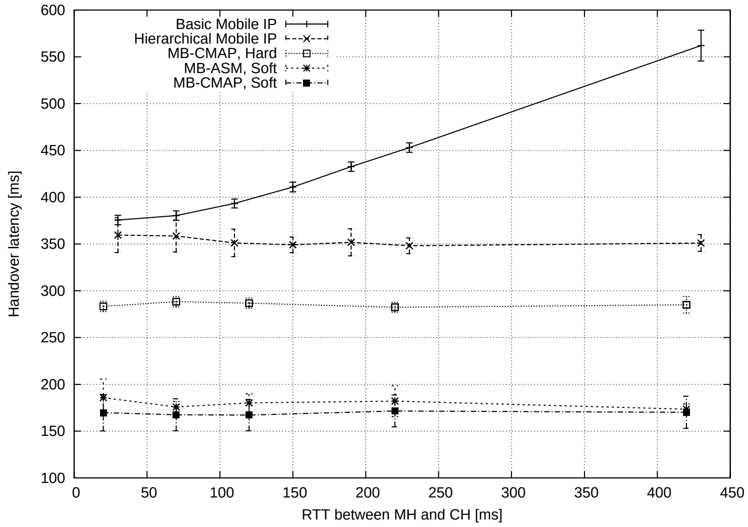
Regarding the handover latency $T_{\mathrm{HO\_Lat}}$, Fig. 8.33 and 8.34 show that the handover latency $T_{\mathrm{HO\_Lat}}$ for the multicast-based schemes remains constant over the RTT, whereas the handover latency for basic Mobile IP increases linearly. The handover latency of hierarchical Mobile IP shows the same behavior as the multicast-based schemes, however, $T_{\mathrm{HO\_Lat}}$ of the multicast-based schemes is even smaller: For advertisement-based trigger $T_{\mathrm{HO\_Lat}}$ of MB-CMAP (hard handover), MB-ASM (predictive handover), and MB-CMAP (predictive handover) is by 70 ms smaller than for hierarchical Mobile IP. The handover latency for MB-CMAP and MB-ASM with soft handover is about 150 ms smaller than for hierarchical Mobile IP. The handover latency can be decreased to less than 150 ms for MB-ASM and MB-CMAP by means of link-layer trigger (Fig. 8.33(b) and 8.34(b)). Comparing the case studies MB-CMAP and MB-ASM, it can be seen that the MB-CMAP has a slightly lower handover latency for soft handover.

Considering the packet loss for UDP traffic (Fig. 8.35(a)), the basic Mobile IP has the highest packet loss with about 38 packet per handover whereas the packet loss is decreased to about 25 packets for hierarchical Mobile IP. Soft handover of MB-ASM and MB-CMAP decreases the packet loss to less than the half (about 15 packets). For the predictive handover of MB-ASM and MB-CMAP no packet loss was observed (not shown in Fig. 8.35).

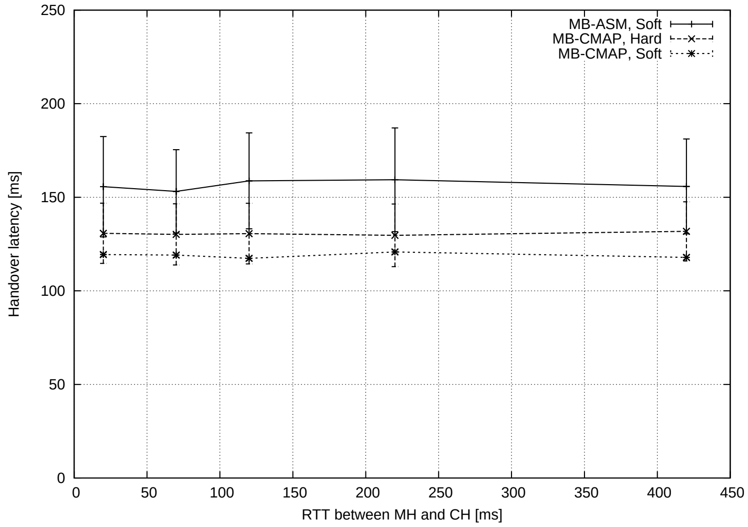
The packet duplication for the predictive handover policy of MB-ASM and MB-CMAP is drawn in Fig. 8.36. For basic and hierarchical Mobile IP no packet duplication was observed; whereas the curves for the predictive policy of both MB-ASM and MB-CMAP show the typical behavior with a steep rise and a shallow slope as explained in Sect. 8.3.2 and 8.4.2. Both curves in Fig. 8.36(a) and 8.36(b) are nearly identical, expect that the inflection point of the curve for MB-CMAP predictive handover is sharper than for MB-ASM predictive handover.

Comparing the results of the relative throughput B_{Rel} for a short-lived TCP connection with a single handover during the ongoing TCP connections the following statements can be made: For advertisement-based trigger (AI = 100 ms) B_{Rel} of the multicast-based schemes and basic and hierarchical Mobile IP is almost identical. (Fig. 8.37(a) and 8.38(a)). For advertisement-based trigger (AI = 1 s) B_{Rel} is reduced to about 0.95 for the soft handover policy of MB-ASM and the hard and soft handover policies of MB-CMAP (Fig. 8.37(b)), whereas B_{Rel} is about 0.9 for basic and hierarchical Mobile IP. In comparison with the advertisement interval of 100 ms, the higher latency for handover detection caused by the larger advertisement interval is nearly compensated by the soft handover policy of MB-ASM and MB-CMAP. For predictive handover (MB-CMAP and MB-ASM) B_{Rel} is improved in comparison with basic and hierarchical Mobile IP (Fig. 8.38(b)). However, there is no significant improvement in comparison with MB-ASM and MB-CMAP soft handover. For link-layer trigger in comparison with an advertisement-based trigger with $AI = 100\ ms$ no improvement is observed.

Considering long-lived TCP connections with multiple subsequent handovers it can be stated that with an advertisement interval of 100 ms the soft and hard handover policy of MB-ASM and MB-CMAP have comparable performance in comparison to basic and hierarchical Mobile IP. (Fig. 8.40(a)) The predictive handover policy of MB-CMAP slightly improves B_{Rel} of basic and hierarchical Mobile IP, whereas predictive handover of MB-ASM shows similar performance (Fig. 8.41(a)). With an advertisement interval of 1s the soft handover policy of MB-ASM and MB-CMAP considerably improves B_{Rel} (Fig. 8.40(b)). The predictive handover policy of MB-ASM and MB-CMAP improves B_{Rel} (Fig. 8.41(b)). The improvement is, however, smaller than the improvement of the soft handover policy of MB-ASM and MB-CMAP. The usage of link-layer trigger improves the TCP throughput slightly.

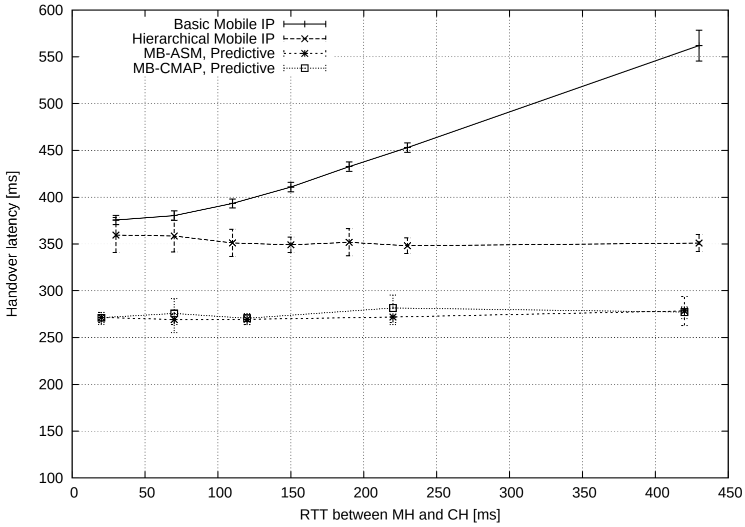


(a) Hard and soft handover, advertisement-based trigger

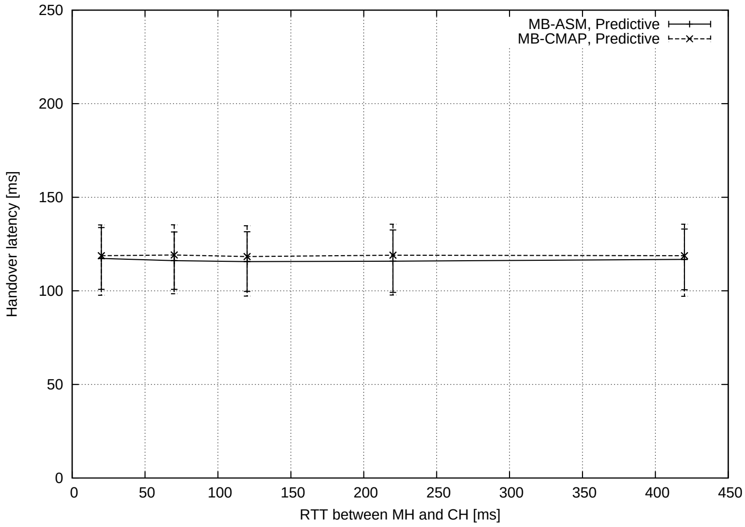


(b) Hard and soft handover, link-layer trigger

Figure 8.33.: Comparison of the case studies and the reference case: Handover latency versus RTT between CH and MH for hard and soft handover (Measurements with 99 % confidence)

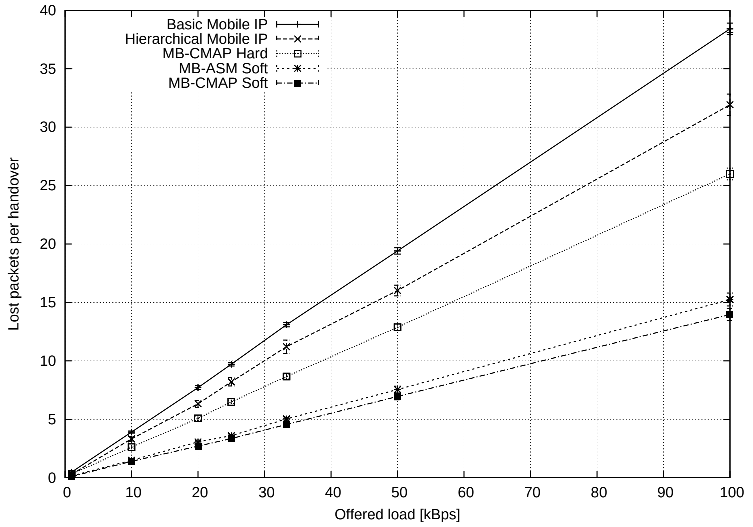


(a) Predictive handover, advertisement-based trigger

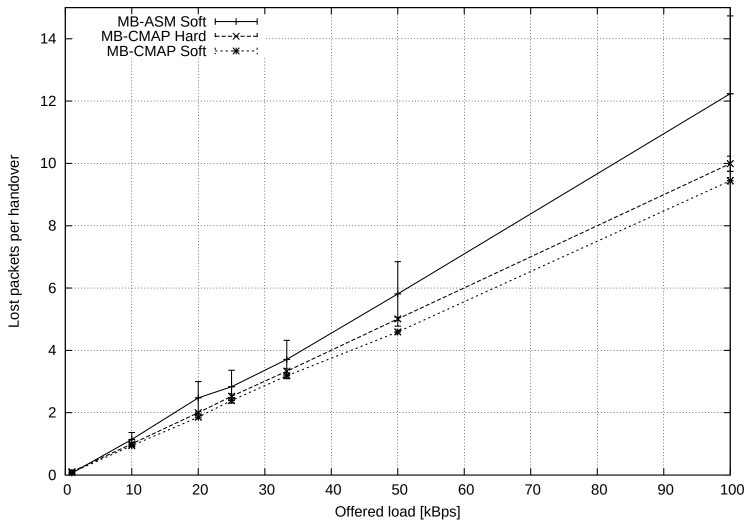


(b) Predictive handover, link-layer trigger

Figure 8.34.: Comparison of the case studies and the reference case: Handover latency versus RTT between CH and MH for predictive handover (Measurements with 99 % confidence)

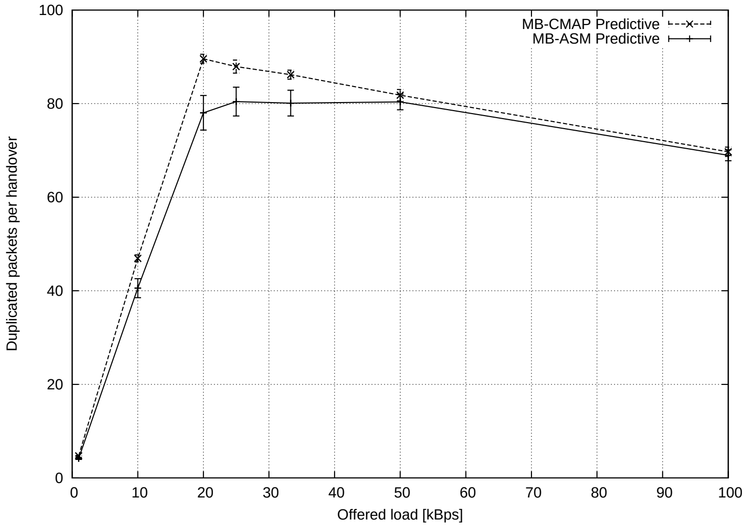


(a) Hard and soft handover, advertisement-based trigger

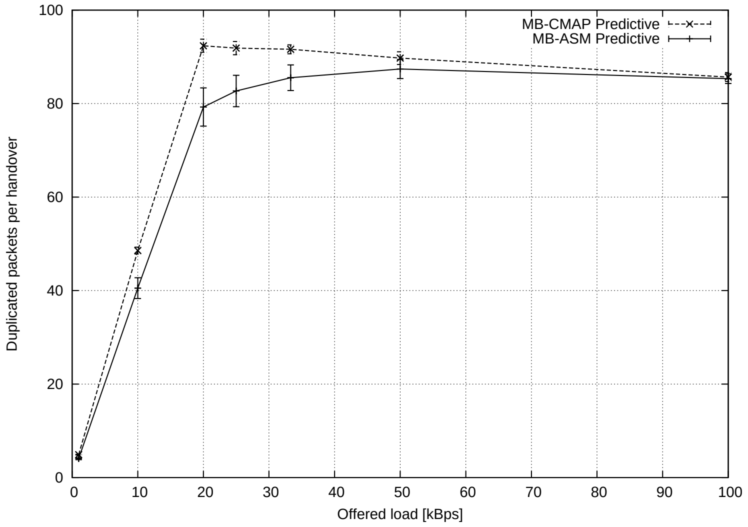


(b) Hard and soft handover, link-layer trigger

Figure 8.35.: Comparison of the case studies and the reference case: Packet loss versus offered load (Measurements with 99 % confidence)

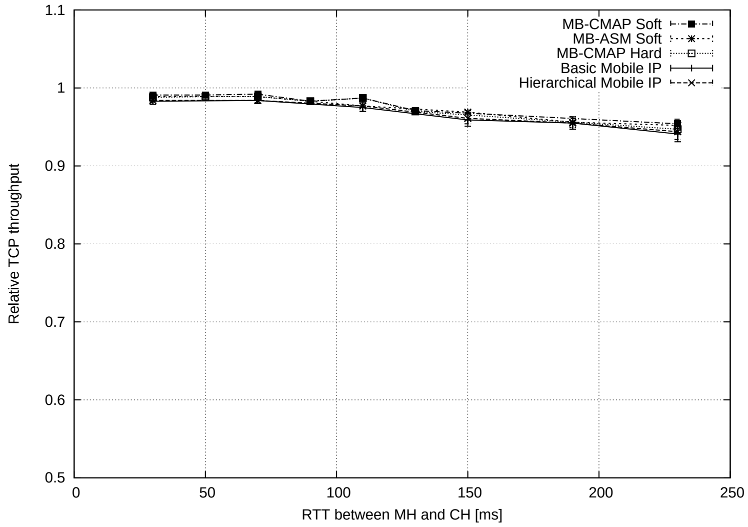


(a) Predictive handover, advertisement-based trigger

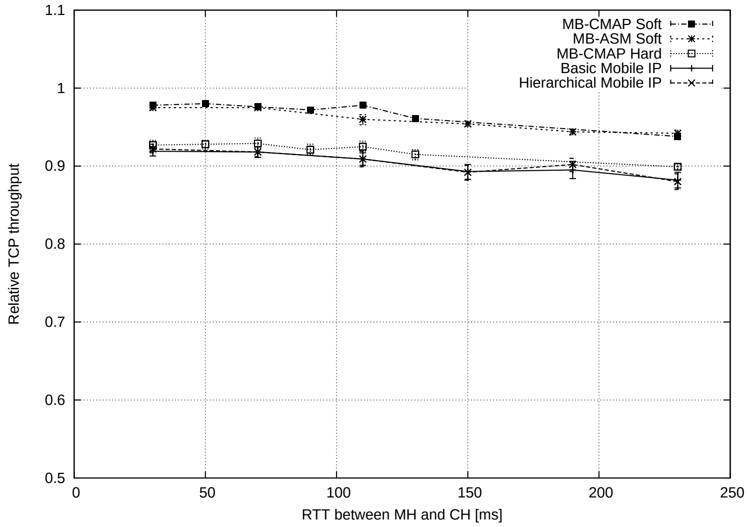


(b) Predictive handover, link-layer trigger

Figure 8.36.: Comparison of the case studies and the reference case: Packet duplication versus offered load (Measurements with 99 % confidence)

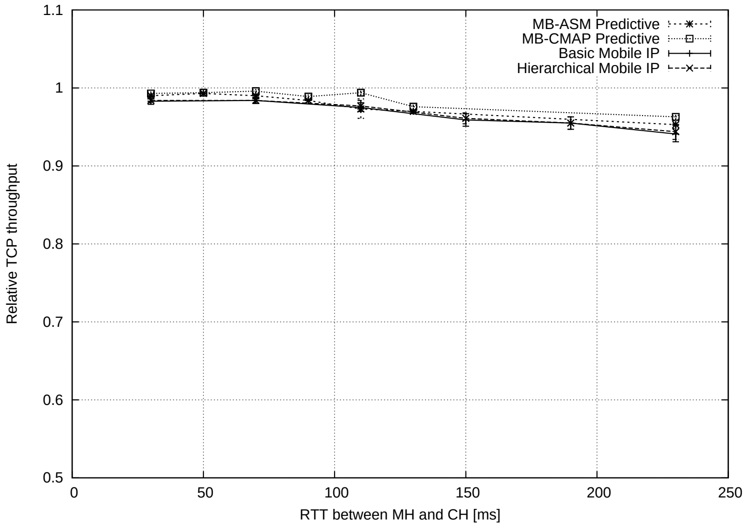


(a) Hard and soft handover, advertisement-based trigger (Advertisement interval = 100 ms)

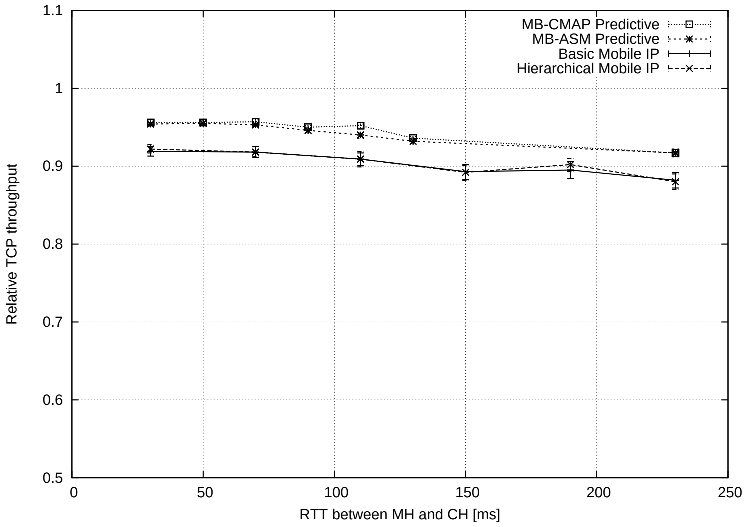


(b) Hard and soft handover, advertisement-based trigger (Advertisement interval = 1 s)

Figure 8.37.: Comparison of the case studies and the reference case: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover for hard and soft handover with advertisement-based trigger (Measurements with 99 % confidence)

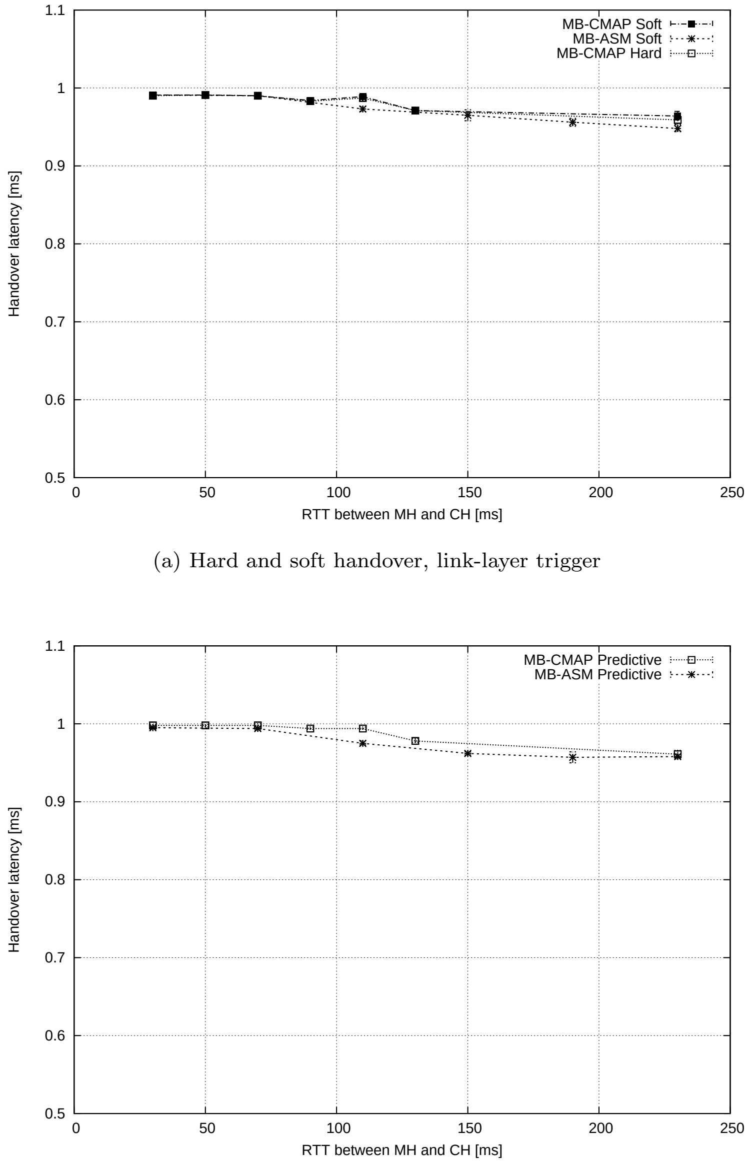


(a) Predictive handover, advertisement-based trigger (Advertisement interval = 100 ms)



(b) Predictive handover, advertisement-based trigger (Advertisement interval = 1 s)

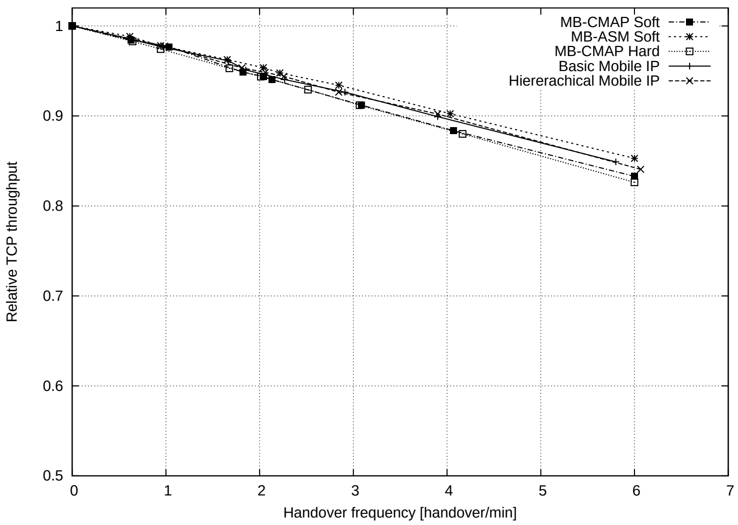
Figure 8.38.: Comparison of the case studies and the reference case: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover for predictive handover with advertisement-based trigger (Measurements with 99 % confidence)



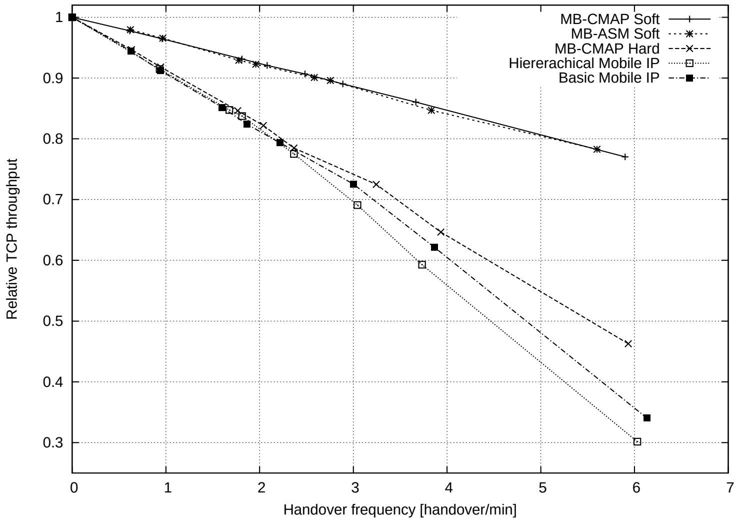
(a) Hard and soft handover, link-layer trigger

(b) Predictive handover, link-layer trigger

Figure 8.39.: Comparison of the case studies: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover for hard, soft and predictive handover with link-layer trigger (Measurements)

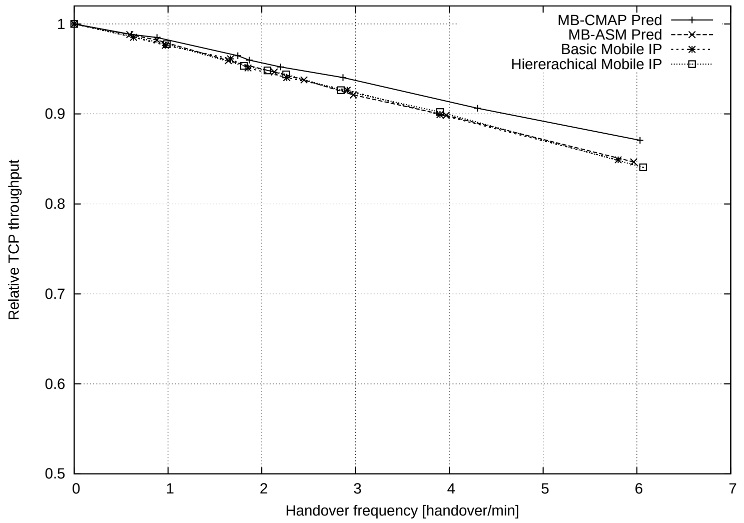


(a) Hard and soft handover, advertisement-based trigger (Advertisement interval = 100 ms)

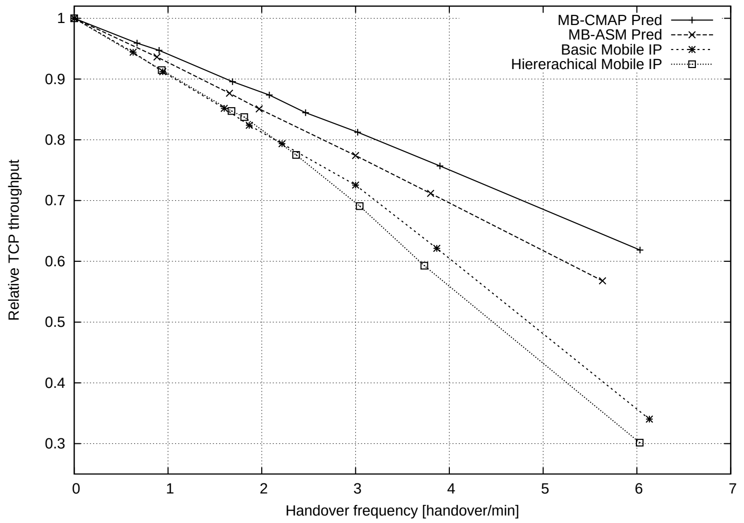


(b) Hard and soft handover, advertisement-based trigger (Advertisement interval = 1 s)

Figure 8.40.: Comparison of the case studies with the reference case: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers for hard and soft handover with advertisement-based trigger (Measurements)



(a) Predictive handover, advertisement-based trigger (Advertisement interval = 100 ms)



(b) Predictive handover, advertisement-based trigger (Advertisement interval = 1 s)

Figure 8.41.: Comparison of the case studies with the reference case: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers for predictive handover with advertisement-based trigger (Measurements)

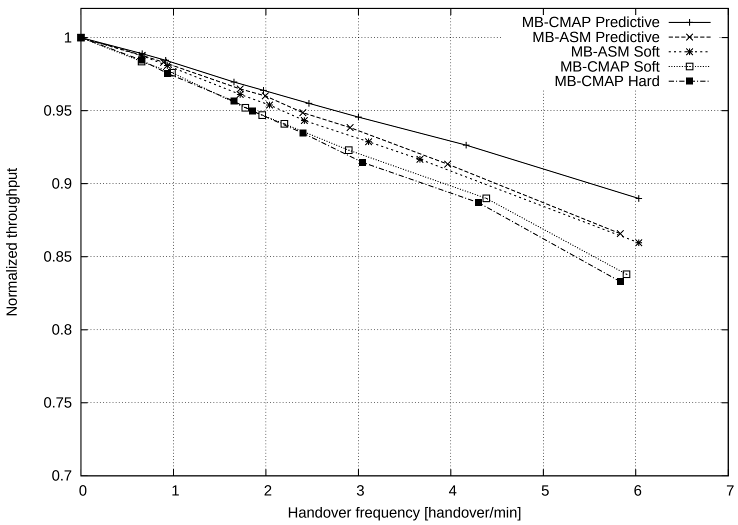


Figure 8.42.: Comparison of the case studies: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers for hard, soft, and predictive handover with link-layer trigger (Measurements)

The following figures compare the case study MIP-SGM with the reference case basic and hierarchical MIP. With respect to the measurement results, the simulation model gives a more optimistic estimation of the handover performance than the measurement model. This is described in Appendix B where the simulation and measurement results of basic and hierarchical Mobile IP are compared.

Fig. 8.43 shows that the handover latency of SGM-enhanced basic Mobile IP and SGM-enhanced hierarchical Mobile IP is reduced by about 100 ms relative to basic and hierarchical Mobile IP. This reduced handover latency corresponds directly with reduced losses as shown in Fig. 8.44, where at an offered load of 100 kBps the packet loss of MIP-SGM is about 10 packet smaller than of the reference case.

Considering the TCP throughput of a short-lived TCP connection with a single handover, B_{Rel} is almost identical for advertisement-based trigger with an advertisement interval of 100 ms (Fig. 8.45(a)), except for a very high RTT between the mobile and correspondent host (e.g. $\approx 450\ ms$). For an advertisement interval of 1 s, the SGM-enhanced schemes improves the TCP throughput considerably (between 5 % and 10 %, Fig. 8.45(b)). Taking into account that multiple handovers impact each other, then the TCP throughput of basic and hierarchical Mobile IP degrades. The SGM-enhanced schemes improve the TCP throughput by about 20 % (SGM-enhanced basic Mobile IP) and 25 % (SGM-enhanced hierarchical Mobile IP).

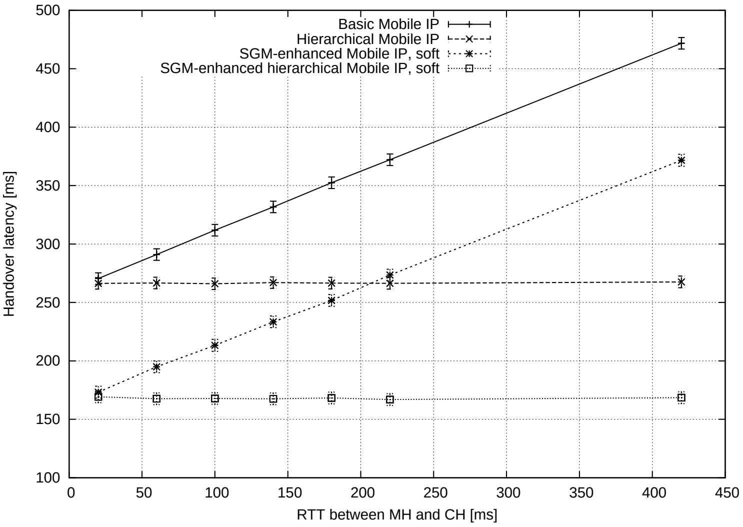


Figure 8.43.: Comparison of the case study MIP-SGM and the reference case: Handover latency versus RTT between CH and MH (Simulation with 99 % confidence)

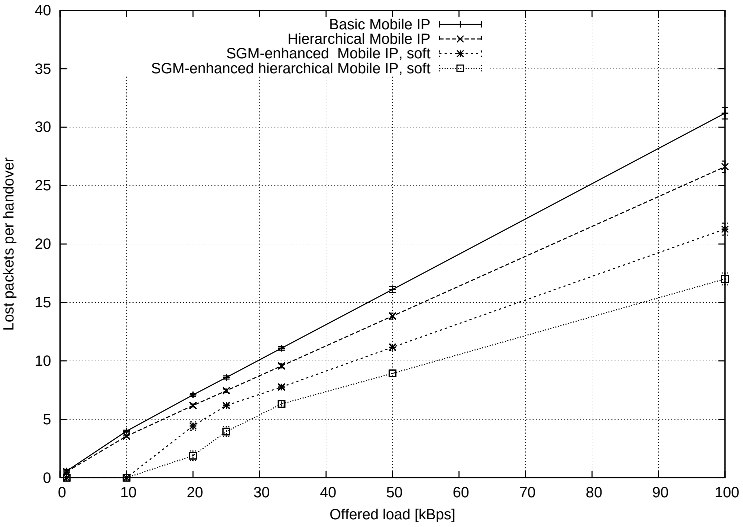
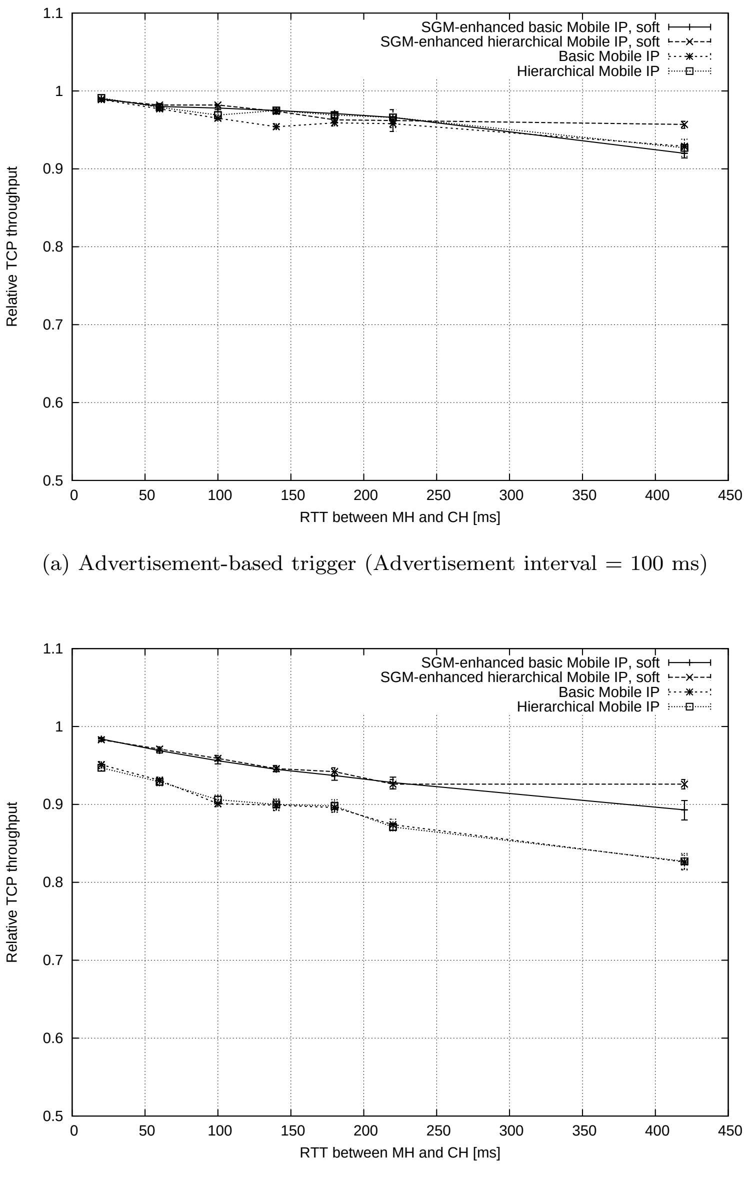


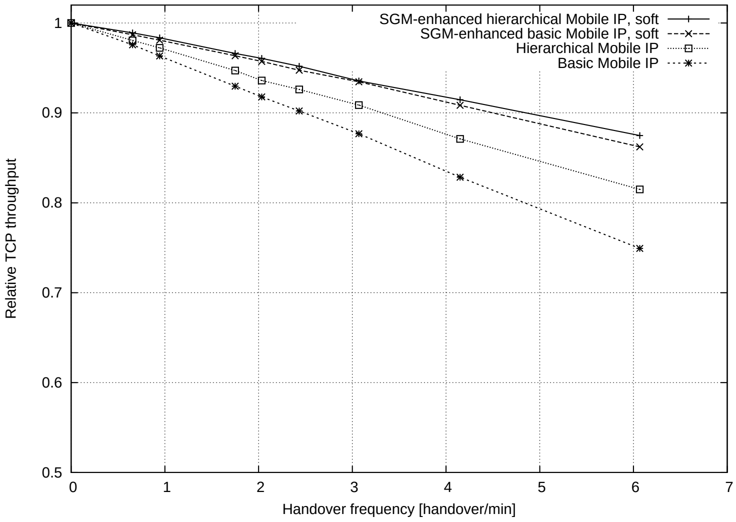
Figure 8.44.: Comparison of the case study MIP-SGM and the reference case: Packet loss versus offered load (Simulation with 99 % confidence)



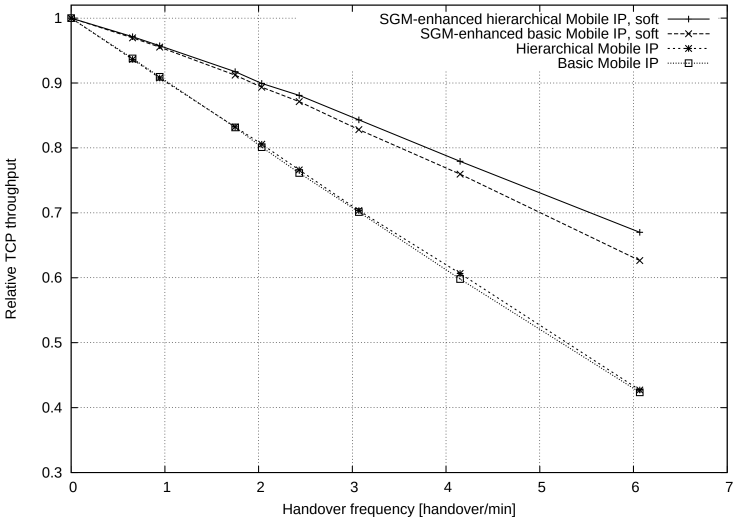
(a) Advertisement-based trigger (Advertisement interval = 100 ms)

(b) Advertisement-based trigger (Advertisement interval = 1 s)

Figure 8.45.: Comparison of the case study MIP-SGM with the reference case: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover with advertisement-based trigger (Simulation with 99 % confidence)



(a) Advertisement-based trigger (Advertisement interval = 100 ms)



(b) Advertisement-based trigger (Advertisement interval = 1 s)

Figure 8.46.: Comparison of the case study MIP-SGM with the reference case: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handovers with advertisement-based trigger (Simulation)

8.7. Scalability

In this section scalability issues for the selected case studies are discussed. Two main scalability concerns can be identified: The *first* concern is the scalability with the number of mobile hosts. The *second* concern is about routers that interconnect an access network with the internet and represent a concentration point of state information as well as signaling and data traffic.

Address allocation, the amount of multicast state and if signaling are aspects that potentially limit the scalability.

Address allocation. A well-known limitation of the IP ASM service model is the number of available multicast addresses in IP version 4 and the need for global address allocation. Using the ASM model, overall less than 300 million class D IP addresses are available which limits the provisioning of a global multicast service. For allocation of a global address, several approaches exist (see Sect. 3.2.1), however, the SSM model leverages the address allocation problem by identifying a multicast group by a source address and a receiver group address (channel). In the case studies MB-ASM and MB-SSM the multicast addresses have to be allocated in a particular access network. Therefore, for address allocation a local procedure is used and the multicast address assigned to a mobile host is locally scoped within the access network. Consequently, the multicast packets remain in the access network and are not forwarded out of the access network. Due to the usage of multicast in the access network, the address allocation problem is solved for these case studies. In the case study MB-CMAP, the *call id* is allocated by means of local mechanisms as well. In the case study MIP-SGM, a mobile host is assigned a unicast address, and hence, no multicast addresses at all need to be allocated.

Multicast state. Unlike unicast routing, the routing of multicast packets in IP networks does not rely on aggregated routing: Every multicast group has a separate entry in the forwarding table of every router along the path. Since the multicast addresses are topologically independent, they cannot be mapped to the hierarchical design of the Internet. The usage of the same mechanisms for aggregated routing as for unicast routing is not possible.[9] In order to estimate the amount of multicast state per multicast router, it can be assessed first that a multicast group is created per mobile host. Then, it can be stated, that the routing state for *explicit-join* multicast routing protocols as used for the case studies MB-ASM scales with $O(R)$ (see also Tab. 3.1), whereas *broadcast and prune* multicast routing protocols scales with $O(SxR)$. In the case studies MB-ASM, MB-SSM, and MB-CMAP the state information in a network node grows linearly with the number of mobile hosts in the network. The state information exists in every router along the path from the gateway to the mobile hosts. Considering the case study MIP-SGM, the routing state is part of the unicast routing table: In the foreign and home agents the routing entries determine tunnel endpoints and result in per-mobile entries in the routers executing an foreign or home agent.

Signaling overhead. *Signaling costs* are defined as the product of weighted hops signaling messages and the signaling rate:

$$\text{Signaling costs} = \text{Weighted hops} * \text{Signaling messages} * \text{Rate}$$

The signaling costs reflect the consumption of communication bandwidth and their processing in the network, as well as the consumption of battery power in the mobile hosts. The signaling costs for the reference case and the case studies are analyzed in Appendix C using the simple

[9] Nevertheless, aggregation of multicast routing state is the subject of ongoing research efforts, e.g. [79, 153]

network model described in Sect. 5.2.3. The signaling costs of the case studies are increased in comparison to the reference case basic and hierarchical Mobile IP. A detailed analysis of the signaling overhead for a particular topology of an access network can be found in Appendix C. The signaling overhead as well as the amount of multicast state in the routers can be reduced by the support of idle connectivity of mobile hosts and paging.

The costs of the idle connectivity is a deferred delivery of packets of newly established data streams generated by a correspondent host. In an experiment, this delay was measured by sending single *ICMP echo requests* to a mobile host in the inactive state. The duration between sending the first ICMP echo request and receiving the corresponding ICMP echo reply gives the round trip time including the paging delay. For the case study MB-ASM an interesting behavior could be observed: The mean paging delay of 100 observations amounts to about 1.2 seconds with a standard variation of about 0.5 seconds. The histogram for the paging latency is depicted in Fig. 8.47 and shows peaks at multiples of 0.5 seconds. The reason for this shape is the polling algorithm to notify the multicast forwarding cache of a successfully resolved multicast entry. In detail, after the paging request was sent and the paging daemon has received a paging update, the entry in the multicast forwarding cache is marked as unresolved.[10] This triggers a cache miss report to the multicast routing daemon. The multicast routing daemon is polled until the routing entry for the corresponding mobile host could be resolved. The polling interval is set to 0.5 seconds by the used *Linux* kernel. This is a reasonable value taking into consideration that the polling is done per multicast group and the number of mobile hosts can be high. It is well-known that polling is an inefficient mechanism and alternative mechanisms would likely give better results. Nevertheless, the polling mechanism has been used since it requires only minimal changes in the multicast routing demon and kernel support itself. The high delay opens some potential for improvement. However, the paging latency applies to the first packet(s) of a newly established data stream only. For most applications, this paging delay is acceptable.

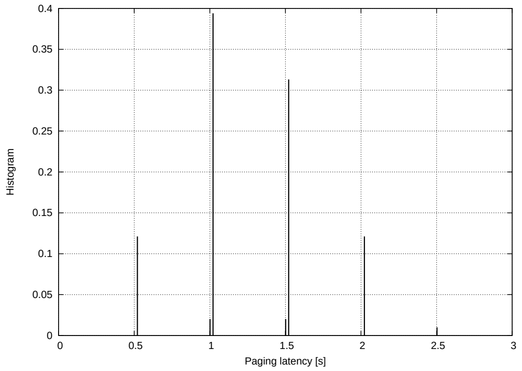


Figure 8.47.: MB-ASM: Histogram for the RTT of an ICMP echo request/reply including the paging delay

[10] This is the usual mechanism to resolve a multicast routing entry which is not in the routing cache.

8.8. Summary of the Evaluation

In this chapter the selected approaches were evaluated and their performance compared. For experimental investigation a common evaluation environment was designed that has allowed an examination of all schemes under comparable experimental conditions. After describing the experimental setup for each case study, a set of experiments were conducted, the performance results presented and analytically validated. Considering the performance results, the following conclusion can be drawn.

The case study MB-ASM offers a soft and a predictive handover policy. In combination with advertisement-based handover trigger, the *soft handover policy* reduces the service interruption of the basic Mobile IP by more than 200 ms (by about 400 ms in the case of very high RTT between the mobile host and the correspondent host/home agent) and of the hierarchical Mobile IP by 200 ms. The packet loss for UDP traffic corresponds directly with the service interruption and is reduced accordingly to about 15 packets at an offered load of 100kBps, whereas under the same experimental conditions with basic and hierarchical Mobile IP more than double of the packet loss was observed. The *predictive policy* provides a lossless handover for UDP traffic, i.e. in the investigated scenario with even non-overlapping cells packet loss was completely avoided. As a tradeoff, the handover latency of the predictive handovers policy is higher than for soft handover, but still by more than 50 ms smaller than for hierarchical Mobile IP. Also, the predictive handover causes a considerable packet duplication for UDP traffic (maximum 80 duplicated packets in the investigated scenario). Since these packets are sent over the wireless link, the duplication of packets can be regarded as a serious drawback. Nevertheless, the proposed solution offers space for optimization to reduce the overhead (see the outlook in Sect. 9.2).

Regarding TCP traffic for soft and predictive handover with advertisement-based handover trigger, the TCP throughput of basic and hierarchical Mobile IP is only improved for a high handover latency, e.g. caused by a high latency for handover detection with an advertisement interval of 1 s (by about 8 % in comparison to basic and hierarchical Mobile IP for short TCP connections of 60 s with a single handover). Particularly, long-lived TCP connections with multiple and frequent handovers benefit from the usage of soft handover: The relative TCP throughput B_{Rel} is reduced only to about 0.8, whereas B_{Rel} of basic and hierarchical Mobile IP degrades to less than 1/3.

The case study MB-CMAP provides a hard, soft, and predictive handover policy. Each of the policy represents a certain tradeoff between the handover performance and the overhead in terms of used resources. Hence, the case study MB-CMAP provides more flexibility in providing handover policies to mobile hosts than the case study MB-ASM. The handover performance of MB-CMAP soft and predictive handover policy is very similar to the performance of the case study MB-ASM soft and predictive handover, respectively in terms of handover latency, UDP packet loss as well as TCP throughput. The hard handover policy of MB-CMAP provides a similar handover latency as the predictive policy that is still smaller than the basic and hierarchical Mobile IP case. The hard handover policy also causes packet loss (yet about one third less than the basic Mobile IP in the investigated scenario), but does not suffer from the packet duplication of the predictive policy. Therefore, the hard handover policy represents a useful complement to the predictive and soft handover policy and meets different application requirements than the soft and predictive handover policy. However, the hard handovers policy requires third-party signaling as a functionality offered by the underlying multicast policy, whereas this functionality is not offered by the case study MB-ASM. Since there are only marginal performance differences between MB-ASM and MB-CMAP for soft and predictive handover, the hard handover policy can be regarded as the benefit from using the advanced features of the CMAP/CMNP multicast approach that increases the flexibility.

For the case study MB-SSM it was assumed that it provides the same handover performance as the case study MB-ASM. The assumption could be made since the underlying multicast policy of both case study is *protocol-independent multicast (PIM)*, whereas for handover in MB-SSM the same functionalities are used as in MB-ASM except the rendezvous-point functionalities for shared trees. However, the main benefit of the case study MB-SSM lies in reduced implementation and deployment complexity and improved security.

The case study MIP-SGM improves the handover performance of basic and hierarchical Mobile IP. The SGM-enhanced policies reduce the handover latency of basic and hierarchical Mobile IP by about 100 ms. The UDP packet loss is decreased by about 10 packets and the relative TCP throughput improved by 20 % (SGM-enhanced basic Mobile IP) and 25 % (SGM-enhanced hierarchical Mobile IP).

The gain of MIP-SGM is comparable to other case studies MB-ASM, MB-SSM, and MB-CMAP, whereas one of the main benefits of the multicast-based approach is constricted: Although MIP-SGM reuses a multicast-based infrastructure[11], the SGM multicast policy is limited to multicast services with small groups. In contrast to MB-ASM, MB-SSM, and MB-CMAP, the case study MIP-SGM still relies on the Mobile IP infrastructure. Hence, the provision of multicast services to mobile host is more complex and causes the problems as described in Sect. 3.2.1.

In addition, the following statements can be made that arise from general questions:

Buffering and forwarding of packets for TCP traffic. It was shown by measurements that for UDP traffic a lossless handover can be achieved by means of predictive handover in the case study MB-ASM and MB-CMAP. For TCP traffic, however, the predictive handover policy improves the TCP throughput of basic and hierarchical Mobile IP, but in comparison with the soft handover the TCP throughput is worse. The reason for this behavior is the reaction of TCP on the duplication of TCP data segments acknowledgements, respectively. The reaction of TCP on a combination of slow start and subsequently received duplicated data segments results finally to a reduced throughput. On the one hand, it can be concluded that predictive handover does not improve the TCP throughput. On the other hand, it is well known that standard TCP shows a bad performance over wireless links. A modified TCP can provide a better performance, however, this is the subject of ongoing research efforts. The question, whether a predictive handover policy with buffering and forwarding of packets is a promising option for a modified TCP is an open question (see the outlook in Sect. 9.2)

Vertical handover. The experiments with vertical handover have shown, that there is no significant difference between the handover performance of vertical and horizontal handover. Two limitations of the experiments must be taken into account: First, in the experimental setup both interfaces in the mobile host are equal. In reality, different interfaces in the mobile host are more typical, such as a wireless LAN and a Bluetooth interface with technology-specific characteristics. For example, it was observed by measurements that the time for re-association at an access point with a Bluetooth interfaces is higher than for a wireless LAN interface. Second, the experimental setup does not take into account that the route from the correspondent host to the new interface of the mobile host can be considerably longer after a vertical handover. This increases the overall handover latency for soft handover and depends on the topology of the backbone network. Both effects are not taken into account by the measurements. Nevertheless, the experiments have shown, that switching the interface in the mobile host during the vertical handover has no considerable impact on the handover performance.

Scalability. Principally, for multicast-based mobility support three potential scalability concerns can be identified. First, the need for global allocation of multicast addresses is one of main scalability issues for multicast services in fixed networks. Due to the limitation of the case

[11] The routers the network must support SGM.

studies to micro-mobility this issue does not limit the scalability. Second, in each router that belongs to the multicast tree, multicast state exists. The selected multicast routing protocol results in one routing entry per multicast group (and hence per mobile host) in that routers. Although commercial multicast routers support typically multiple of 10.000 routes, this remains an potential scalability limitation for access networks with a very high number of mobile hosts. Third, it has been shown in Appendix C that multicast schemes results in a higher signaling overhead in terms of (weighted hops * signaling messages). In this context it could also be seen that the support of inactive mobile hosts and paging significantly reduces the signaling overhead. Clearly, the amount of the signaling overhead depends on the activity behavior of users and applications.

9. Conclusions and Outlook

In this dissertation the challenge of supporting host mobility in IP cellular networks is addressed. It is argued that the today's cellular communication networks offer seamless mobility support but are based on a homogeneous networking technology and a complex, voice-oriented networking infrastructure. Internet technology is expected to cause a paradigm shift in cellular communication networks. The Internet architecture, protocols, and applications provide flexible services with heterogeneous networking technology at prospectively lower costs. Nevertheless, the IP protocols lack the support of host mobility. The dichotomy of the IP address (its meaning as a host identifier as well as the host's location in terms of its network point of attachment) can be identified as the basic reason. The classical solution to overcome this problem is Mobile IP. This solution assigns a temporary IP address in addition to the IP address that this host would have in its home network. Packets are routed indirectly via the home network to the current network point of attachment by means of tunneling. This solution has been widely criticized for its drawbacks including the triangular routing and its effect on protocol overhead and end-to-end delays, router ingress filtering, and handover performance.

In this dissertation a different approach is pursued that solves the general mobility problem by means of multicast. Taking a simplified view, data destined to the mobile host are efficiently distributed to multiple locations in advance of handover. When the mobile host executes a handover to one of the locations, data are already available and can immediately be forwarded. Principally, this can be achieved by the capability of multicast for location-independent addressing and routing. The mobile host gets assigned a multicast group address and joins the multicast group at different locations. A multicast distribution tree is set up and the tree branches reach the current as well as expected locations of the mobile host on its move. The branches of the multicast tree grow and shrink and follow the mobile host's footprint. In comparison to Mobile IP, the multicast-based mobility support provides the following advantages: *First*, re-routing for handover is executed in the network node where the paths to the old and from the new access point diverge (and not in a software agent in the mobile host's home network as in the Mobile IP approach). *Second*, a handover-specific signaling and infrastructure is in principle not required, instead multicast is reused for mobility purposes. And *third*, multicast offers handover mechanisms that can be utilized in a flexible manner to provide the desired service quality as a tradeoff between service interruption, packet loss and protocol overhead.

It has already been recognized that multicast offers a number of attractive features for mobility support, particularly in highly mobile environments with very small cells. Nevertheless, the utilization of multicast for mobility support poses a number of challenges that have been insufficiently addressed so far: First of all, multicast does not offer all functionalities that are required or useful for mobility-related performance. Also, the today's IP multicast faces a number of open problems, even in fixed networks. Other challenges arise from the usage of multicast for mobility support, such as the scalability with the number of multicast groups. Several interesting proposals in this area have already been made with different motivations, requirements, and assumptions about the networking architecture.

In the dissertation the requirements for multicast-based support of host mobility are identified as well as mobility functions and basic protocol options elaborated. The three components create a framework for the system and protocol design of multicast-based mobility support that is termed MOMBASA (**Mo**bility Support – A **M**ulticast-**Bas**ed **A**pproach). The framework is used to judge existing research approaches and serves as a basis to design new schemes and modify existing ones. Four case studies based on different multicast service models are derived from the framework. The first case study (MB-ASM) uses the classical any-source multicast (ASM) service model of IP with a dynamic, open, and anonymous group of receivers. The second case study (MB-SSM) is based on a single-source multicast (SSM) service model. The service model has the same features as ASM, but restricts the number of sources for the tree, and therefore leverages several drawbacks of the ASM service model. The third case study (MB-CMAP) employs the multi-point, multi-connection call (MCall) service model which dynamic, closed, non-anonymous groups. It allows a fine-grained management of the members of multicast groups and of the communication between their members. The fourth case study is based on the explicit multicast (XCast) service model. The service model is optimized for small group and meets the requirement of multicast-based mobility support by being scalable with the number of groups with only a few group members. Since the small group multicast (SGM) does not rely on location-independent addressing and routing, but basically on unicast communication, the SGM is utilized to improves the basic mobility schemes basic and hierarchical Mobile IP, resulting in case study MIP-SGM.

The four case studies are considered as potential candidates for multicast-based mobility support. They rely on a set of basic protocol options that are common and different in each of the case studies. For example, in all case studies the end point of the mobile host is located in the access point, while the underlying multicast service model is different. Likewise, some options of the mobility functions are common to all case studies while others specifically utilize the capabilities of the multicast protocol. Based on the definition of the case study, a set of protocols are designed that augment the particular multicast.

The methodology of investigation is a combined approach of measurements, simulation, and analysis. For experimental investigation, the *MOMBASA Software Environment*, a generic software platform for experimentation with multicast-based mobility support in IP-based networks is developed. The software environment offers an abstract interface to the multicast, and hence can be used for future investigations of different classes and types of multicast. The *MOMBASA Software Environment* is part of the evaluation environment that allows to investigate the selected case studies and the reference case in a common experimental environment under comparable conditions.

This results of the investigation show the feasibility of a mobile communication system with multicast-based mobility support providing the full spectrum of IP services. Potential problems of multicast-based mobility support (e.g. lack of a reliable transport service for multicast, ARP problems by using multicast addresses, etc.) can be avoided. Measurements in an experimental testbed have shown that the handover performance of multicast schemes are at least comparable to basic Mobile IP in terms of handover latency, packet loss and TCP throughput. The support of multicast-based host mobility facilitates a high degree of flexibility in the provision of handover: Different handover policies can be provided that are designed to meet the different application requirements with respect to service interruption, packer loss, and protocol overhead. The soft handover provides a very short service interruption by setting up multicast tree branches to the old and the new access point simultaneously during the handover and by reducing the duration to detect the handover. The predictive handover provides a lossless handover. With the predictive handover policy branches are set up to multiple access points in advance of handover. These access points buffer data and forward the buffered data when the mobile host registers. Finally, the hard handover minimizes the protocol overhead caused by handover. The handover policies can be used dynamically chosen by the mobile host according to selected requirements, such as service interruption, losses, protocol overhead, costs, and other criteria.

The investigation of different case studies in this dissertation has shown that for multicast-based mobility support only a subset of the ASM service model is used. It could be shown that the SSM service model is ideally suited to the topology of an access network. The SSM service model also offers a reduced implementation and deployment complexity as well as improved security while achieving a performance that is comparable with that of more complicated multicast models. Since the benefits of the SSM service model have been recognized for fixed networks, the advantages can be confirmed for the utilization of multicast for mobility, though for other reasons. While for fixed networks the improved address allocation, address allocation, scalability, and charging are the main reasons of using the SSM service model, it is mainly the implementation and deployment complexity as well as improved security that makes the SSM service model the better choice. The MCall service model enables a better control of the access points that belong to a mobile host's multicast group and the data transport to these access points, including third party signaling. These features facilitate more flexibility in provisioning of handover policies than the ASM service model. Although it is shown that these features do not result in an improvement of the handover performance, the features eases the management of mobility and network-topology-specific information, and therefore simplifies protocol design and deployment complexity. The XCast service model in the case study MIP-SGM does not imply the multicast-specific overhead since it does not need any multicast routing protocol and multicast routing state in the network, but is, however, tied to the existing Mobile IP mechanisms.

Finally, this dissertation examines scalability aspects that represent concerns for multicast-based mobility support. The basic issues that potentially limit the scalability are the need for global address allocation, the number of multicast state and the increased signaling overhead. The usage of multicast for micro-mobility supersedes the necessity of a global address allocation. The application of explicit-join protocols for multicast routing instead of broadcast–and–prune protocols results in per-mobile routing entries in multicast routers, whereas today's commercial multicast routers can handle multiple 10.000 entries. The signaling overhead for multicast-based mobility support is indeed higher than for basic and even hierarchical Mobile IP, but it was shown that the signaling overhead (and the number of multicast states in the access network) can be considerably decreased by the support of inactive mobile host and paging. The signaling cost analysis has given the ratio of active and inactive mobile host where the signaling costs of the case studies equal the reference case Mobile IP.

From the performance evaluation two additional statements can be made. First of all, it could be seen that the usage of multicast for mobility support shortens the service interruption due to handover, but using advertisement-based handover trigger a seamless handover can only be achieved when advertisement are sent with a high frequency considerably increasing the protocol overhead. The main reason is that the multicast-based mobility support does not reduce the duration to detect a handover. The usage of link-layer trigger is necessary to achieve further improvements. Also, the performance evaluation has shown that the TCP throughput does not strongly benefit from multicast-based mobility. Therefore, the conclusion can be drawn that the multicast-based mobility support does not supersede the enhancement and adaption of TCP for mobile environments.

The success of a future mobile communication system providing multicast-based mobility support is strongly associated with the success of the multicast in general in future IP networks. The multicast service model and multicast protocols that will be used depends on how these approaches overcome the problems of the today's classical ASM service model. Potential candidates were evaluated in this dissertation and it could be shown that not a single perfect multicast exists. Without being committed to multicast protocols as existent today, a multicast-based mobility support would highly benefit from several multicast features: Single source multicast and multicast with closed groups is ideally suited for the topology of an access network and improves the security. Non-anonymous groups simplify the management of a multicast tree for soft and predictive handover and facilitates the resource reservation in advance and the sub-casting of data to a subset of access points for predictive handover.

9.1. Contributions

The major contributions of the dissertation are:

1. The dissertation proposes a wireless mobile system architecture that re-uses a multicast infrastructure for mobility purposes. The proposal attempts to utilize a multicast service as it will likely be offered in future IP networks without modifying the multicast scheme itself for mobility purposes.

2. The dissertation provides a framework for the design of multicast-based mobility support. This framework elaborates the multicast-specific requirements for mobility support and identifies mobility functionalities and general design options for protocols. The framework serves as a basis to design new schemes and modify existing solutions for multicast-based mobility support. In the dissertation, four case studies were derived from the framework. These case studies differ in the multicast service model and other basic system and protocol options as well as mobility functions utilizing specific features of the multicast. The case studies explicitly incorporate alternative multicast schemes, that are not based on the classical ASM service model of the Internet.

3. For the selected case studies of multicast-based mobility support a set of protocols is designed. A software platform was developed from which prototypes for the selected case studies are created.

4. A common environment for performance evaluation was designed that allows the investigation of the selected case studies as well as the reference case under comparable experimental conditions.

5. Within the dissertation, a policy driven approach for mobility support was developed. The approach allows to control mobility-related system behavior and resources. By means of policies, a mobile host can choose a handover scheme according to the application requirements and the consumed resources (protocol overhead).

6. The handover performance of the selected case studies for multicast-based mobility support was quantitatively evaluated. The performance was compared with the traditional approach of mobility support in IP networks (Mobile IP and the variant hierarchical Mobile IP).

7. As one of the major results, for multicast-based mobility support an alternate service model than the classical ASM model is advocated. The main benefits of the SSM service model lie in reduced implementation and deployment complexity and improved security while achieving a performance that is comparable with that of more complicated multicast models. The MCall service model facilitates a fine-grained control of group membership and communication resulting in a great flexibility of handover policies, whereas the XCast model can be employed to improve the handover performance of the Mobile IP approach without incurring any of the overhead caused by multicast management and routing protocols.

9.2. Outlook

A number interesting research questions arise from this dissertation:

Investigation of mobile multicast. This dissertation considers multicast schemes that were originally designed for wire-line networks with fixed hosts and utilizes its capabilities for mobility-support without modifying the multicast schemes. This is achieved by augmenting the multicast schemes with mobility-specific functionalities by means of complementary protocols. An alternative approach worth considering is the design of a multicast scheme that already inherits both multicast and mobility functionalities. The benefit of this approach is that a mobile multicast services can be provided directly to mobile host.

Interaction of mobility enabling proxies (MEPs) and performance enhancing proxies (PEPs). Protocol proxies perform a number of task in IP networks. In this dissertation the usage of mobility-enabling proxies for support of host mobility was proposed. Performance Enhancing Proxy (PEP)s [22] are often employed to improve degraded TCP performance caused by characteristics of specific links, for example, in satellite, wireless WAN, and wireless LAN environments. For the design of PEPs several proposals exist (e.g. ReSoA [142]), whereas the simultaneous applications of both types of proxies in a network – and even an integration – is an open challenge. Closely related to this issue is the question for performance of enhanced TCP with multicast-based mobility: Within this dissertation the performance of standard TCP with multicast-based mobility support was investigated. Since standard TCP interprets packet loss due to handover as network congestion, it invokes the TCP congestion control and avoidance mechanisms and un-necessarily reduces the TCP throughput. Several alternative TCP approaches have been proposed. These extensions attempt to improve the TCP throughput in spite of mobility. A combined evaluation of multicast-based mobility support and a TCP variant for mobile environments can give more accurate results of the handover performance seen by applications that use TCP as a transport protocol.

Provision of link-layer trigger for handover in a heterogeneous networking environment. Handover detection and triggering are important handover functionalities that contribute significantly to the overall service interruption caused by handover. As shown in this dissertation, the usage of link-layer trigger has a strong impact on the overall handover performance. A link-layer trigger for handover is an alternative to a network layer trigger. It reduces the time to detect and trigger handover by means of cross-layer information from the link layer to the network layer. Link-layer information such as signal strength may be continuously available and thus can be measured at any frequency, providing valuable information about the present link quality. Link-layer information may therefore allow a mobile node to detect the loss of connectivity more quickly than a network layer advertisement-based algorithm. In some cases, link-layer information may be used to detect a decaying wireless link before the link is broken. This facilitates the execution of the handover and the elimination of the time to detect handover. However, the usage link-layer trigger for handover in a heterogeneous networking environment causes a dependence of the IP layer from the underlying technology. The development of a generic interface for information exchange between the link layer and the network layer for different link-layer types (or at least for certain classes of different link layers, e.g. wireless LAN-like) avoids the development of a multitude of specific protocol stacks that would aggravate and hamper the deployment of heterogeneous all-IP wireless networks.

Security problems in multicast-based mobility support. Mobile networks are by nature more vulnerable as far as security is concerned. The usage of multicast for mobility makes authentication, authorization, and data integrity a challenging problem [114]. The provision of a secure multicast service even in non-wireless IP networks is the subject of ongoing research efforts (e.g. [114, 160]). In general, security for multicast communication is more problematic since it requires a securely distributing a cryptographic key to all members of the multicast group. The usage of multicast-based mobility support has specific requirements to a secure multicast service, such as a small size of multicast groups with typically a few members only in a highly dynamic multicast group with frequent joins and leaves. Another specific condition of a secure multicast-based mobility support is the employed multicast type. As it was elaborated within this dissertation, a source-specific multicast solves the problem of traffic from unwanted sources in the any-source model by restricting the sources to a single host. Regarding receiver and authentication and authorization, it simplifies the key distribution protocol in comparison to the any-source multicast model. A secure multicast service support represents a pre-requisite for a successful multicast-based mobility service.

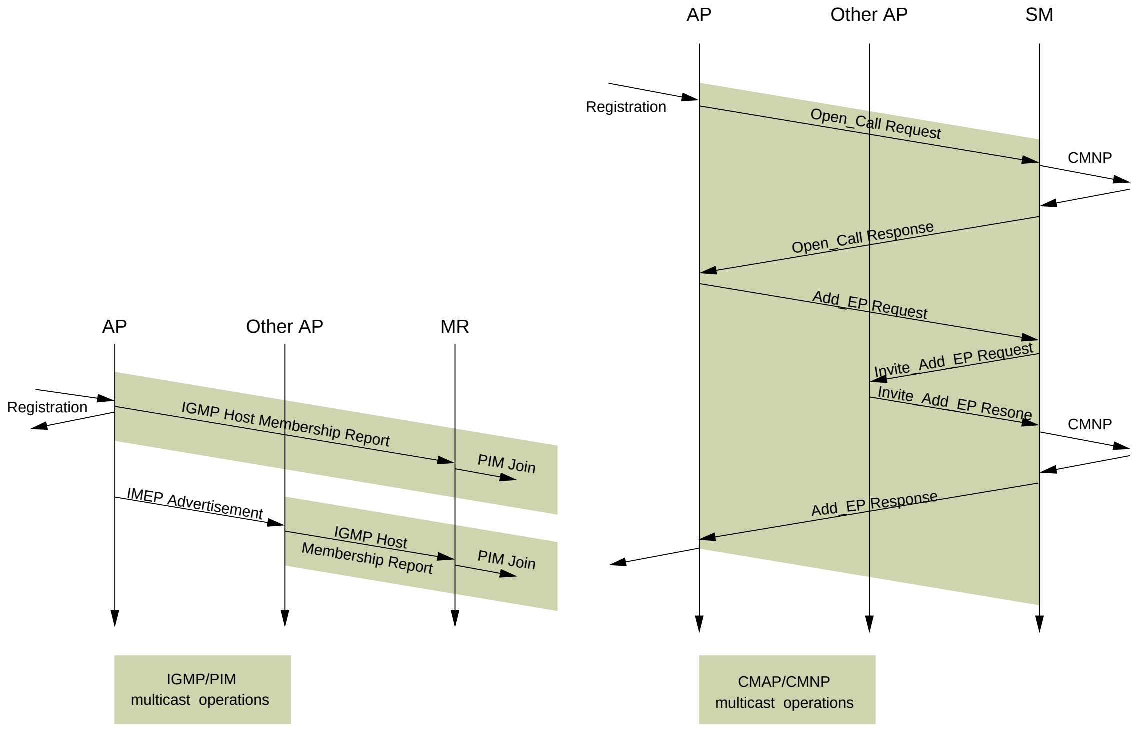
9.3. Final Remarks

In recent years, cellular networks have emerged as networks that provide voice applications as well as data applications at low data rates. Inevitably, mobile networks will be interconnected to the Internet accommodating more diversified applications than today's mobile networks. To continue the success of the Internet even in wireless and mobile environment, a paradigm shift from voice-oriented technology of today's mobile networks to an Internet architecture and IP-based protocols is needed. While the today's cellular networks with a homogeneous wireless technology provide seamless handover, in future IP-based cellular networks the diversified application requirements ranging from stringent demands for seamless or lossless handover to more relaxed requirements must be met in an efficient fashion. *Mobile IP* as the traditional approach to mobility support in IP networks has been widely criticized for offering a single solution that attempts to fit all requirements. *Multicast-based mobility* is an alternative promising approach to the traditional solution to provide a flexible mobility service for hosts in large access networks. It is intended to work in conjunction with other mobility approaches in neighboring access networks and rather complement these mobility approaches than replace them. A step in studying the multicast-based mobility support has been taken that covers the design of protocols, the development of a software prototype, as well as the experimental investigation of different case studies in a common evaluation environment. The path to a prosperous access network that offers a multicast-based mobility service is hard to predict; it also strongly depends on the success of a multicast service in future IP-based networks. The research in this area is of great theoretical interest as well as practical importance.

A. Detailed Protocol Operations of Case Studies MB-ASM, MB-SSM, and MB-CMAP

In Chapt. 6 the protocol design for the case studies MB-ASM, MB-SSM, and MB-CMAP was described by means of generic multicast operations. The following figures incorporate the operations of the particular multicast schemes with more details.

Initial Registration

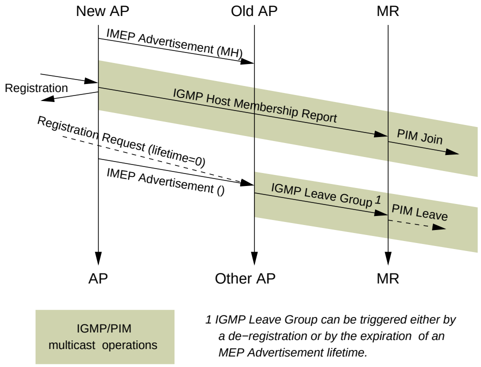


(a) Case studies MB-ASM and MB-SSM

(b) Case studies MB-CMAP

Figure A.1.: Time-line: Registration

Handover



1 IGMP Leave Group can be triggered either by a de−registration or by the expiration of an MEP Advertisement lifetime.

Figure A.2.: Time-line: Soft handover in the case studies MB-ASM and MB-SSM

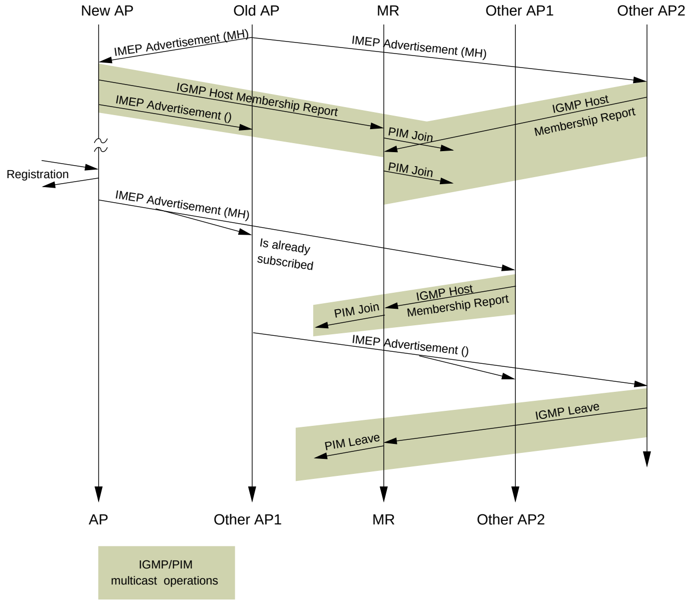
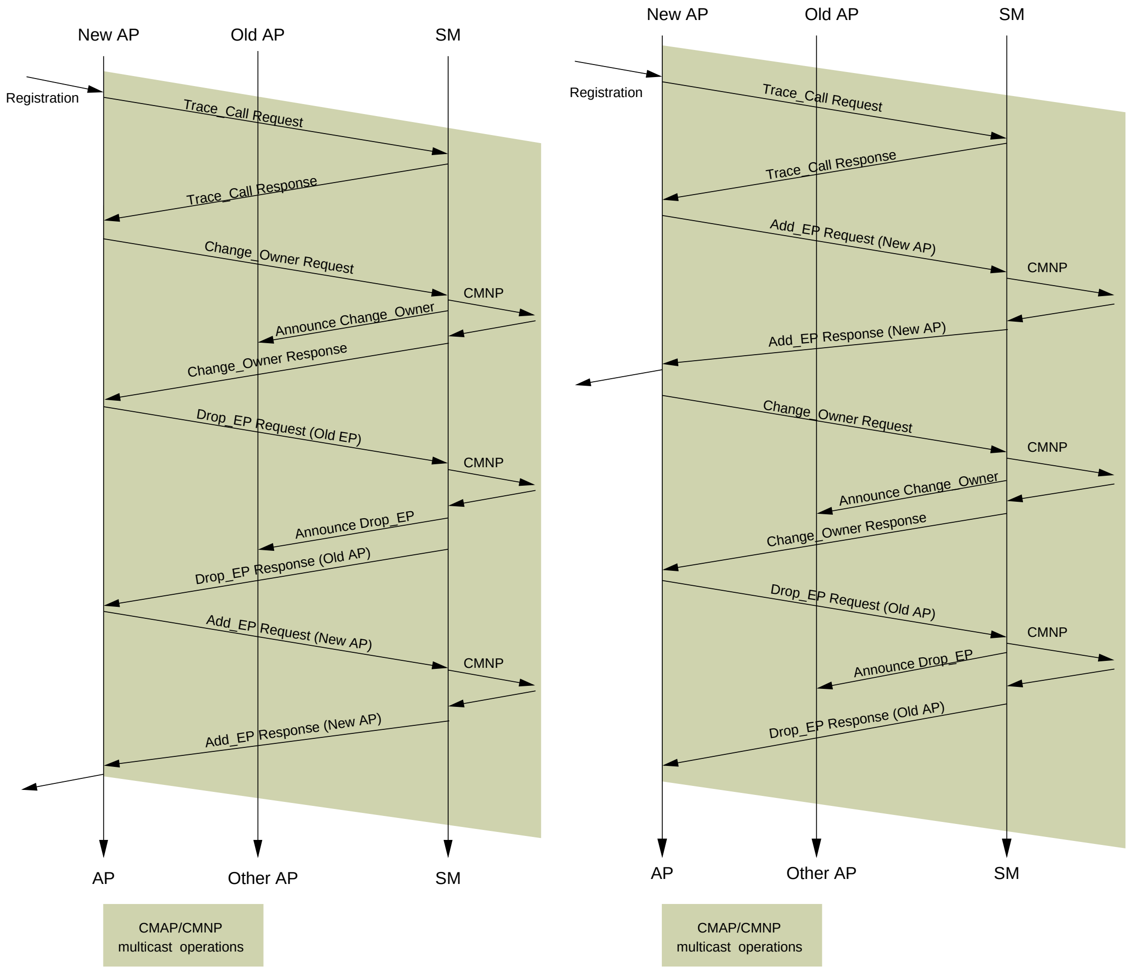


Figure A.3.: Time-line: Predictive handover in the case studies MB-ASM and MB-SSM



(a) Hard handover

(b) Soft handover

Figure A.4.: Time-line: Hard and soft handover in the case study MB-CMAP

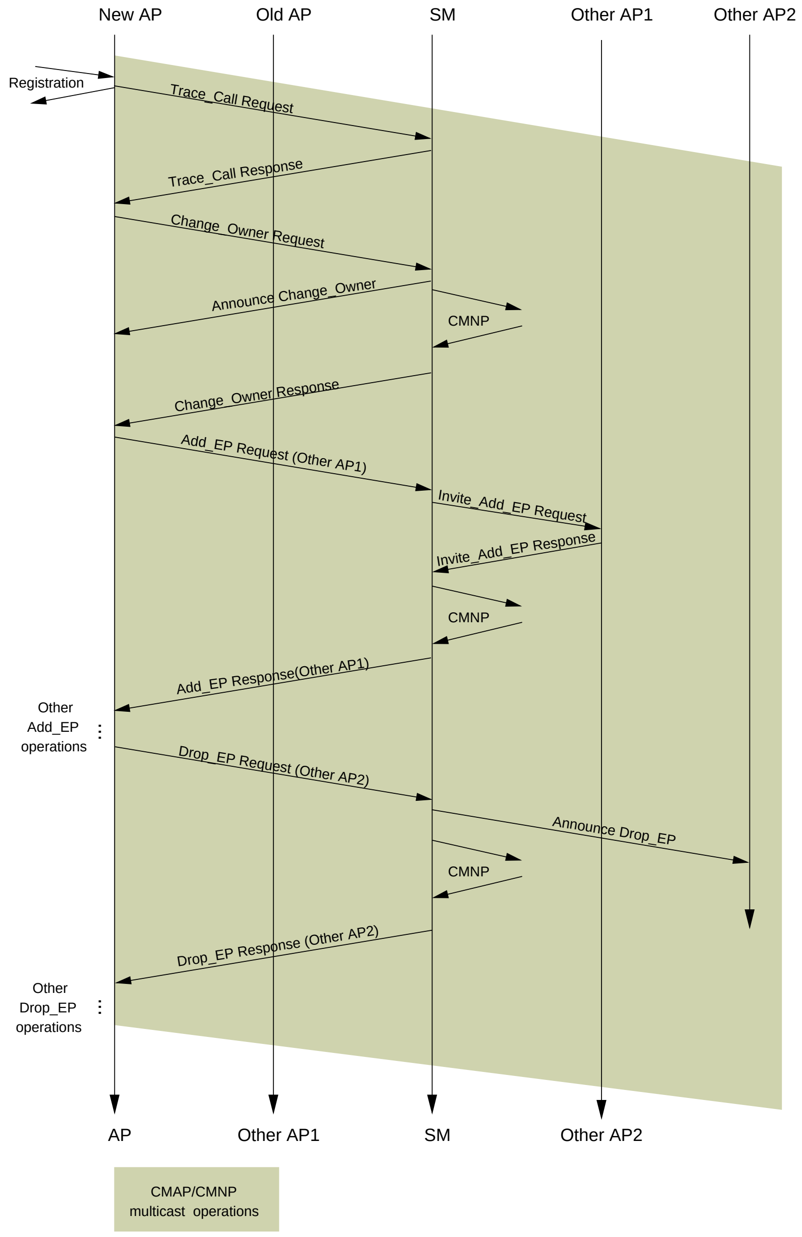
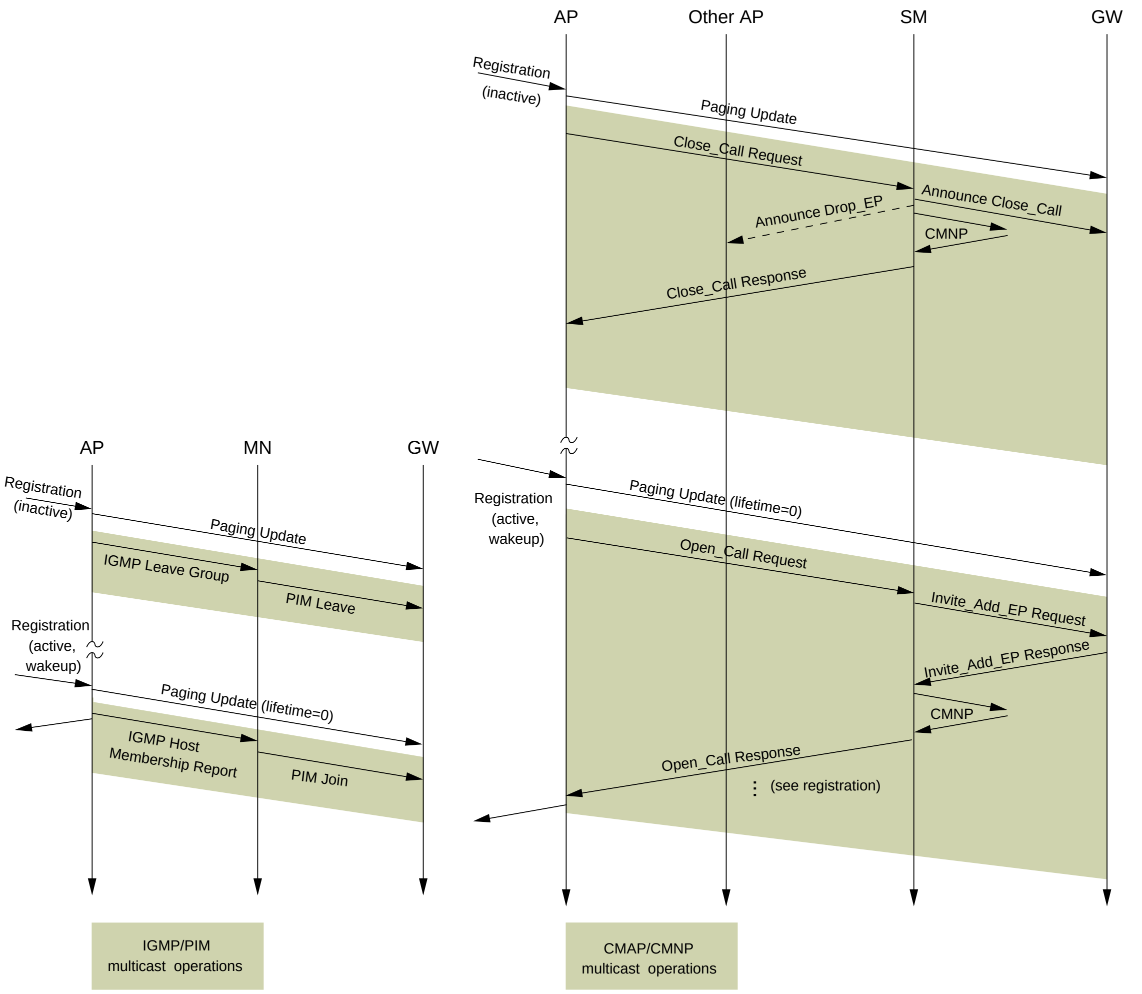


Figure A.5.: Time-line: Predictive handover in the case study MB-CMAP

Switching Between Active and Inactive Mode

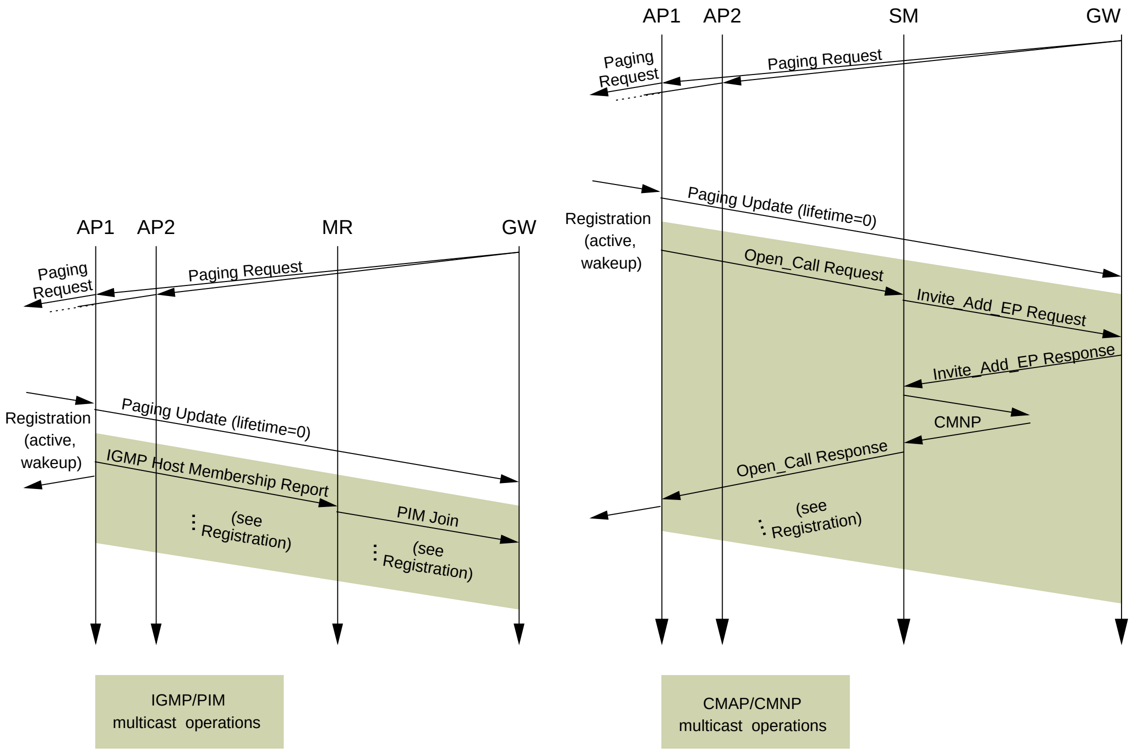


(a) Case studies MB-ASM and MB-SSM

(b) Case study MB-CMAP

Figure A.6.: Time-line: Switching between inactive and active mode

Paging



(a) Case studies MB-ASM and MB-SSM

(b) Case studies MB-CMAP

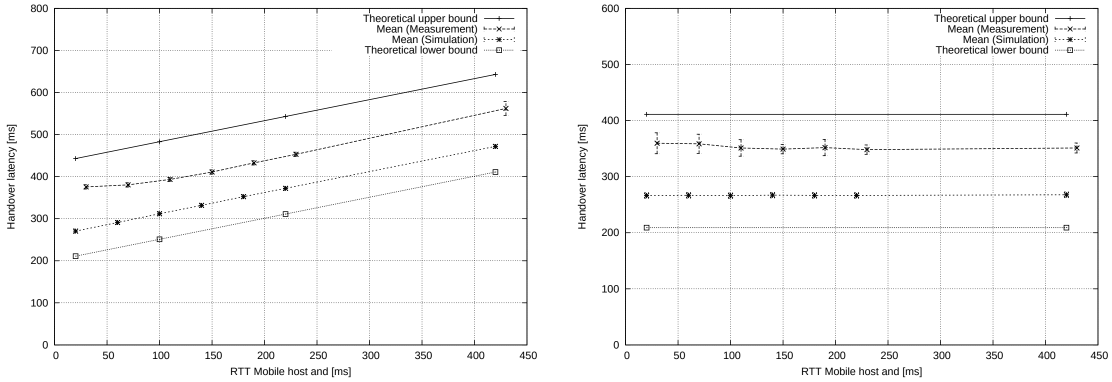
Figure A.7.: Time-line: Paging

B. Comparison of Measurement and Simulation Results for the Reference Case Mobile IP

The performance of the case study MIP-SGM was examined by means of simulation (see Sect. 5.1). The simulation model for MIP-SGM is an extended version of an existing simulation model for basic Mobile IP and hierarchical Mobile IP. The experiments that were conducted with the network model for measurement were repeated by means of simulation. In the following the measurement and simulation results for basic and hierarchical Mobile IP are compared.

Fig. B.1(a) and B.1(b) show that mean handover latency of both measurement and simulation is between the lower and upper bound of analysis. However, the mean handover latency of simulation is by about 80 ms smaller than the measured value for basic Mobile IP as well as for hierarchical Mobile IP. The smaller delay is caused by a difference of the Mobile IP functionality in the mobile host. In the simulation model as well as in the *dynamics* Mobile IP implementation a binding update is sent to the new foreign agent if the advertisement lifetime from the old foreign expires. In the simulation mode the binding update is sent immediately, whereas the *dynamics* implementation works in a slightly different way: Instead of assigning a timer for managing the advertisement lifetimes as in the simulation model, the mobile host manages the advertisement lifetimes in a list. The list is checked for expired advertisement lifetimes when a new advertisement arrives or (if no advertisement is received) frequently in a certain time interval. Hence, in the simulation model the point of time, when a handover is detected and a binding update is sent, is deferred by an additional delay. Since the time interval to check the advertisement list in the mobile host is relatively large (10s of seconds), the deferral is determined by the advertisement interval which was set to 100 ms. However, the management of received advertisements in a list in the *dynamics* Mobile IP implementation can be regarded as an optimization to un-burden the mobile host from timer management and processing when advertisement from many foreign agents are received simultaneously.

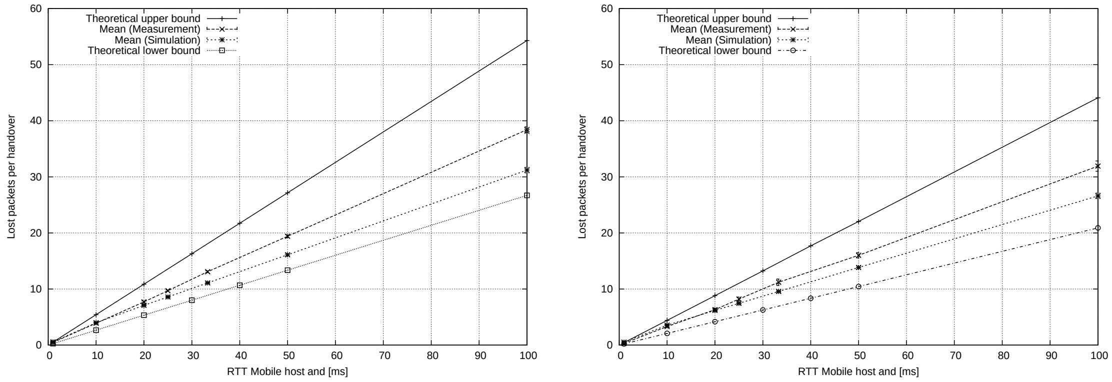
Concerning the handover performance, the simulation model gives an optimistic estimation of the handover latency in comparison with the measurements. Due to this functional difference between the simulation model and implementation, the simulation results of the other metrics show also a better performance, e.g. the packet loss (Fig. B.2(a) and B.2(b)) as well as the relative TCP throughput (Fig. B.3(a)– B.4).



(a) Mobile IP

(b) Hierarchical Mobile IP

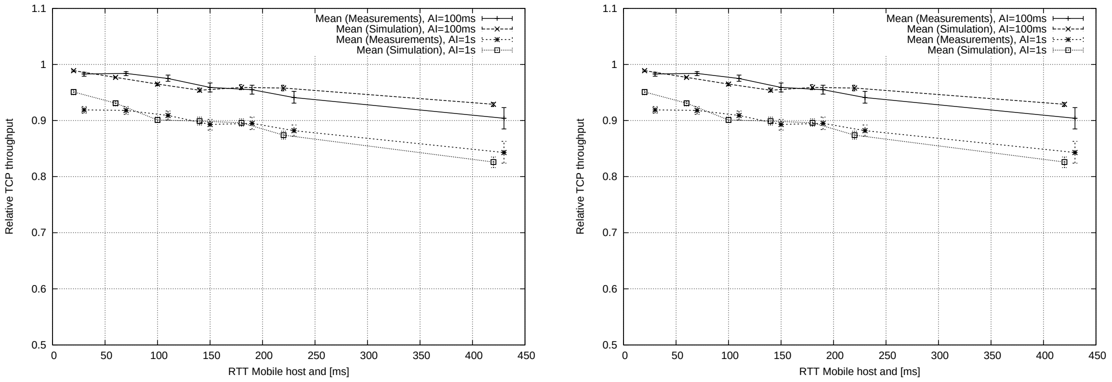
Figure B.1.: Comparison between measurement and simulation results for the reference case basic and hierarchical Mobile IP: Handover latency versus RTT between CH and MH (Advertisement-based trigger)



(a) Mobile IP

(b) Hierarchical Mobile IP

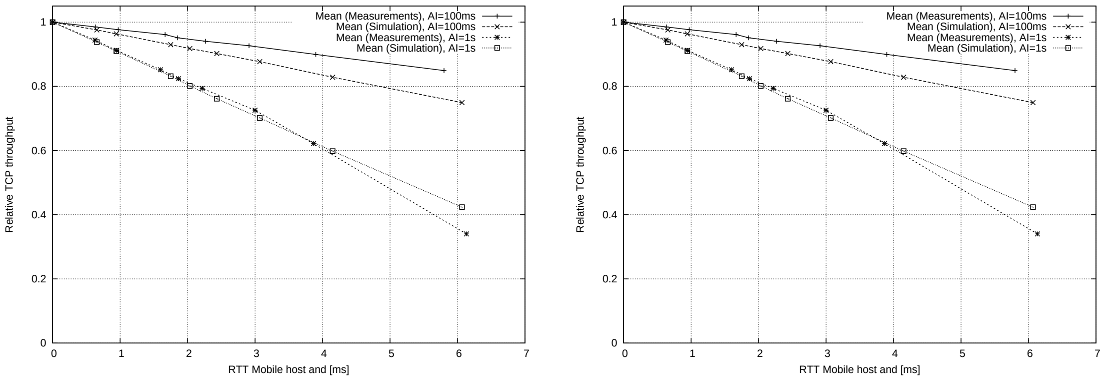
Figure B.2.: Comparison between measurement and simulation results for the reference case basic and hierarchical Mobile IP: Packet loss versus offered load (Advertisement-based trigger)



(a) Mobile IP

(b) Hierarchical Mobile IP

Figure B.3.: Comparison between measurement and simulation results for for the reference case basic and hierarchical Mobile IP: Relative TCP throughput versus handover frequency for a short-lived TCP connection and a single handover (Advertisement-based trigger)



(a) Mobile IP

(b) Hierarchical Mobile IP

Figure B.4.: Comparison between measurement and simulation results for for the reference case basic and hierarchical Mobile IP: Relative TCP throughput versus handover frequency for a long-lived TCP connection and multiple handover (Advertisement-based trigger)

C. Signaling Cost Analysis

In this section the signaling costs for the selected case studies (in each case without paging and then for the paging-enhanced approach) are analyzed.

In general, the signaling costs are comprised of the following components, whereas not all signaling costs pertain to the particular case studies:

1. Advertisements sent by access points on the wireless link to advertise their availability,
2. Advertisements exchanged between access points in order to pre-register mobile hosts for support of predictive handover (if available),
3. Registrations and registration refreshes (re-registrations) sent by the mobile host towards the gateway/home agent,
4. Multicast signaling (membership queries/responses, multicast state refresh messages, etc.),
5. Handover signaling.

In order to calculate the total costs of signaling, only mobility within the access network is considered and signaling outside of the access network is excluded from the analysis. Thus, only local mobility is included. In addition, the following simplification is made for the case studies MB-ASM, MB-SSM, and MB-CMAP: All members of an access point group belong to the same multicast router/switch. Then, the rerouting node (branching point of the multicast tree or switching foreign agent) is the router at the first hierarchical level. In reality, the access points can be attached to arbitrary routers; in the worst case, the rerouting node is the gateway. Also, it is assumed for the case study MIP-SGM, that the switching foreign agent is a router at the first hierarchical level, i.e. the old and new foreign agent are attached to the same foreign agent at the next hierarchical level.

C.1. Definitions and Signaling Costs Common to all Case Studies

First, the following variables are defined that are common to all case studies:

ω_c	Weight of a hop in the fixed segment of the handover domain [ ]
ω_w	Weight of a wireless hop [ ]
$r_{\scriptscriptstyle Adv}$	Rate of advertisements of a MEP/foreign agent $[\frac{1}{s}]$
$S_{\scriptscriptstyle MEPGr}$	Size of an access point group (if predictive handover is supported) [cells]

These variables were already defined in the mobility model described in Sect. 5.3.1:

r_{cc} Cell crossing rate per mobile [1/s] with $r_{\text{cc}} = \eta \frac{v}{R}$ [cells]
δ Density of mobiles in the handover domain $[\frac{1}{m^2}]$
R Cell radius $[m]$
v Velocity of mobile host $[\frac{m}{s}]$
m Number of mobiles in cell with $m = \delta\ \frac{3}{2}R^2\sqrt{3}$ [ ]
η Constant proportional factor for relation between velocity v and cell radius R [ ].

In order to consider paging in the analysis, more variables need to be defined:

α Proportion of active mobile hosts to the overall number of mobile hosts [ ]
s_{PA} Paging area size where the number of cells in the PA is $n_{PA} = 3s_{\text{PA}}(s_{\text{PA}} - 1) + 1$ [ ]
r_{In} Rate of incoming data sessions for a mobile host, equals the paging rate $[\frac{1}{s}]$
r_{Out} Rate of outgoing data session for an idle mobile host $[\frac{1}{s}]$
r_{PU} Rate of paging updates for an idle mobile host where $r_{\text{PU}} = r_{\text{cc}}/(s_{\text{PA}} + \frac{1}{2})$ $[\frac{1}{s}]$

It is common to all case studies that the signaling costs of advertisements contribute with

$$7^3\ \omega_w\ r_{\text{Adv}} \tag{C.1}$$

to the overall signaling costs. The constant (7^3) represents the number of wireless cells in the selected network setup.

The signaling costs of re-registrations sent on the wireless links between the mobile hosts and the access points can be expressed by

$$2\ 7^3\ \omega_w\ m\ r_{\text{Rereg}} \tag{C.2}$$

The multiplier 2 takes into account that a registration operation consists of a request and reply message.

In the next sections the overall signaling costs of the particular case studies are analyzed. The detailed protocol operations are illustrated in Appendix A.

C.2. Signaling Costs for the Reference Case Basic and Hierarchical Mobile IP

The signaling costs for the reference case basic and hierarchical Mobile IP can be simply calculated by the costs of the i) advertisements sent by foreign agents on the wireless link, ii) re-registrations, and iii) handover signaling. The first two components can be calculated by the expressions derived in Eq. (C.1) and (C.2) in Sect. C.1.

The signaling costs for handover are caused by the *Binding_Update Request* and *Response* messages. With basic Mobile IP these messages are sent from the mobile host to the home agent. Due to the limitation of the analysis to the access network boundaries, only the hops within the access network are considered (one wireless and three wired hops). The signaling costs amount to $(2\ 7^3\ (\omega_w + 3\omega_c)\ m\ r_{cc})$. With hierarchical Mobile IP the signaling messages are exchanged between the mobile host and the switching foreign agent, whereas it is assumed that the switching foreign agent is located at the first hierarchical level. Then each signaling message is sent over 2 hops (one wireless and one wired hop). This yields $(2\ 7^3\ (\omega_w + \omega_c)\ m\ r_{cc})$.

The signaling costs are comprised of the components listed in table C.1.

	Expression
Foreign agent advertisements	$7^3\ \omega_w\ r_{\text{Adv}}$
Re-registrations	$2\ 7^3\ (\omega_w + 3\omega_c)\ m\ r_{\text{Rereg}}$
Handover signaling (Basic Mobile IP)	$2\ 7^3\ (\omega_w + 3\omega_c)\ m\ r_{cc}$
Handover signaling (Hierarchical Mobile IP)	$2\ 7^3\ (\omega_w + \omega_c)\ m\ r_{cc}$

Table C.1.: Basic and hierarchical Mobile IP: Analytical results of the signaling costs

C.3. Signaling Costs for the Case Studies MB-ASM and MB-SSM

The calculation of the signaling costs for the case study MB-ASM and MB-SSM is more complex. The specific issues in the calculation of the signaling costs are i) the advertisements exchanged between the access points for support of predictive handover (inter-MEP advertisements), ii) the signaling to refresh the multicast state in the designated routers (IGMP membership queries and responses) as well as in the other multicast routers and the gateway (multicast state refreshes and hello messages of the PIM-SM and PIM-SSM multicast protocol), and iii) the handover signaling.

The following variables specific to the case studies MB-ASM and MB-SSM are defined:

$r_{IMEPAdv}$	Rate of inter-MEP advertisements per MEP $[\frac{1}{s}]$
r_{MQR}	Rate of multicast state refreshes (IGMP membership queries) per link $[\frac{1}{s}]$
r_{PIMR}	Rate of multicast state refreshes (PIM-SM/SSM join/prune messages) per link $[\frac{1}{s}]$
r_{PIMH}	Rate of PIM hello messages per link $[\frac{1}{s}]$

C.3.1. Signaling Costs Without Paging

The signaling costs of advertisements and re-registrations were already calculated in Sect. C.1.

Regarding the inter-MEP advertisements, it is assumed that the messages are first sent uplink from the MEPs to the first multicast router and than distributed down-link to the MEPs of the correspondent MEP group. In contrast, in the case study MB-SSM the inter-MEP advertisements must be sent to the gateway (since the gateway is the only allowed multicast sender). For simplicity in this analysis it is assumed that an inter-MEP advertisement is sent to the gateway and back to the access points, whereas a signaling message is duplicated on the last wired hop to the MEP only. Hence, in a network with a three hierarchical levels, the signaling costs for inter-MEP advertisements can be calculated by $(7^3\ \omega_c\ (\ 5 + S_{\text{MEPGr}}\ )\ r_{\text{IMEPAdv}})$. The term $(5\ +\ S_{\text{MEPGr}})$ takes into account that the active MEP sends the inter-MEP advertisement to the gateway (3 hops) and the gateway forwards the advertisement to the passive MEPs $(2 + S_{\text{MEPGr}})$ hops, whereas the signaling message is duplicated S_{MEPGr} times on the last hop. Then, the term $(7^3\ \omega_c\ (\ 5 + S_{\text{MEPGr}}))$ represents the weighted hops signaling messages that is multiplied with the rate these messages are generated with (r_{IMEPAdv}).

The signaling to refresh the multicast state consists of two components. The first component is signaling traffic caused by IGMP on the links between the access points and their designated multicast routers. A multicast router periodically sends an IGMP *Membership Query* to its attached access points (to the *all host multicast group* 224.0.0.1). An access point answers with an IGMP membership report for each multicast group the MEP belongs to: One per directly registered mobile host (m), one per indirectly registered host ($m\ S_{MEPGr}$) and one per MEP group (S_{MEPGr}) the MEP belongs to. In summary, the signaling costs for IGMP membership queries are ($7^3\ \omega_c\ r_{\text{MQR}}$) and for IGMP membership responses ($7^3\omega_c(m + S_{\text{MEPGr}}m + S_{\text{MEPGr}})\ r_{\text{MQR}}$). The second component represents the messages for multicast state refreshes in the routers (PIM join/prune messages) and the messages for coordination between the multicast routers (PIM hello messages). The periodic PIM join/prune messages carry a list multicast groups to refresh the multicast state amount to ($(7^2\ +\ 7^1)\ \omega_c\ r_{\text{PIMR}}$). The term ($7^2\ +\ 7^1$) represents the number of multicast routers in the access network. The messages of the PIM hello protocol causes a signaling cost of ($(7^2 + 7^1)\ \omega_c\ r_{\text{PIMH}}$).

The costs of handover signaling is comprised of signaling on the wireless links and signaling on the wired links (Fig. A.2 and A.3). The signaling costs on the wireless link can be expressed by ($2\ 7^3\ \omega_w\ m\ r_{\text{cc}}$). The signaling costs on the wired links are different for soft and predictive handover:

- For soft handover the signaling costs between the access points and their designated routers can be calculated by ($2\ 7^3\ \omega_c\ m\ r_{\text{cc}}$). The factor 2 takes into account that an IGMP unsolicited join message and an IGMP leave message (2 messages) are sent.[1]

- The predictive handover causes more signaling costs than the soft handover: The signaling costs between the access points and their designated routers can be calculated by ($6\ 7^3\ \omega_c\ m\ r_{\text{cc}}$), whereas the factor 6 considers that for re-arranging the MEP group six operations are necessary: 3 messages are sent for multicast join operations and 3 messages for multicast leave operations, resulting in 6 signaling messages.

The particular components of the overall signaling costs without paging are listed in Tab. C.2.

	Expression
MEP advertisements	$7^3\ \omega_w\ r_{\text{Adv}}$
Inter-MEP advertisements (predictive)	$7^3\ (5 + S_{\text{MEPGr}})\ \omega_c\ r_{\text{IMEPAdv}}$
Re-registrations	$2\ 7^3\ \omega_w\ m\ r_{\text{Rereg}}$
IGMP membership queries/responses (soft)	$7^3\ \omega_c\ (m + 1)\ r_{\text{MQR}}$
IGMP membership queries/responses (predictive)	$7^3\ \omega_c\ (m + mS_{\text{MEPGr}} + S_{\text{MEPGr}} + 1)\ r_{\text{MQR}}$
PIM state refreshes	$(7^2 + 7^1)\ \omega_c\ r_{\text{PIMR}}$
PIM hello messages	$(7^2 + 7^1)\ \omega_c\ r_{\text{PIMH}}$
Handover signaling (soft)	$2\ 7^3\ (\omega_w + \omega_c)\ m\ r_{\text{cc}}$
Handover signaling (predictive)	$7^3\ (2\omega_w + 6\omega_c)\ m\ r_{\text{cc}}$

Table C.2.: MB-ASM, MB-SSM: Analytical results of the signaling costs without paging support

[1] For simplification we neglect that a multicast router sends an IGMP membership query after an IGMP leave operation to check if other hosts are subscribed to the multicast group.

C.3.2. Signaling Costs With Paging

The signaling costs *with* paging support are composed of the same components as without paging, and additionally of signaling costs for i) *Paging_Update* messages, ii) *Paging_Request* messages, and iii) additional registration messages when mobile hosts change their state. Furthermore, the number of re-registration and handover signaling operations is reduced by the number of inactive mobile hosts. This in turn reduces the number of IGMP membership responses.

The signaling costs of *Paging_Update* messages that are periodically sent by inactive mobile hosts to the gateway amount to $(7^3\ (\omega_w + 3\omega_c)\ (1-\alpha)\ m\ r_{\mathrm{PU}})$. *Paging_Request* messages are sent from the gateway to the access points of the paging area of size s_{PA} and forwarded on the wireless links. Again, the simplifying assumption is made that the access points of the same paging area are attached to a single router of the first hierarchy. Then, the signaling costs of the *Paging_Request* messages amount to $(7^3\ (2\omega_c + s_{\mathrm{PA}}\omega_c + s_{\mathrm{PA}}\omega_w)\ (1-\alpha)\ m\ r_{\mathrm{In}})$. The term $(2\omega_c + s_{\mathrm{PA}}\omega_c + s_{\mathrm{PA}}\omega_w)$ represents the number of weighted links.

A mobile hosts that changes its state from the *inactive* to the *active state* (wake-up) causes a registration message and the multicast signaling necessary that all members join the multicast group (Fig. A.6(a)). For soft handover the signaling costs amount to $(7^3\ (2\omega_w + 6\omega_c)\ (1-\alpha)\ m\ (r_{\mathrm{In}} + r_{\mathrm{Out}})$ for signaling sent on the wireless and the wired links toward the gateway. This results in two signaling messages on the wireless hop (*Registration Request* and *Registration Reply*) and two signaling messages on 3 wired hops (*Paging_Update* message from MEP to gateway - 3 wired hops, *IGMP unsolicited membership report* from the MEP to the multicast router at the first hierarchical level - 1 wired hop, and a *PIM Join* message to the gateway - 2 wired hops). For predictive handover, the signaling costs increase by the costs to add the other access points. This results in $(S_{\mathrm{MEPGr}} - 1)$ additional signaling messages on the links between the access points and the multicast router at the first hierarchical level (1 wired hop).

A mobile hosts that changes its state from the *active* to the *inactive* state, causes a *Paging_Update* message that is sent from the mobile host to the gateway (1 wireless and 3 wired hops) (Fig. A.7(a)). Furthermore, an IGMP leave group message and a PIM leave message are generated (3 wired hops each). It is assumed that the rate these events take place is the same as the rate of incoming and outgoing data sessions $(r_{\mathrm{In}} + r_{\mathrm{Out}})$. Then, the signaling costs in the access network amount to $(7^3\ (\omega_w + 6\omega_c)\ \alpha\ m\ (r_{\mathrm{In}} + r_{\mathrm{Out}}))$

Tab. C.3 summarizes all signaling costs including the paging support.

	Expression
MEP advertisements	$7^3\ \omega_w\ r_{\mathrm{Adv}}$
Inter-MEP advertisements (pred.)	$7^3\ \omega_c\ (5 + S_{\mathrm{MEPGr}})\ r_{\mathrm{IMEPAdv}}$
Re-registrations of active mobile hosts	$2\ 7^3\ \omega_w\ \alpha\ m\ r_{\mathrm{Rereg}}$
Paging updates of inactive mobile hosts	$7^3\ (\omega_w + 3\omega_c)\ (1-\alpha)\ m\ r_{\mathrm{PU}}$
Paging requests	$(7^3\ (s_{\mathrm{PA}}\omega_w + 2\omega_c + s_{\mathrm{PA}}\omega_c)\ (1-\alpha)\ m\ r_{\mathrm{In}}$
State transition Inactive to Active (soft)	$7^3\ (2\omega_w + 6\omega_c)\ (1-\alpha)\ m\ (r_{\mathrm{In}} + r_{\mathrm{Out}})$
State transition Inactive to Active (pred.)	$7^3\ (2\omega_w + 6\omega_c + (S_{\mathrm{MEPGr}} - 1)\ \omega_c)\ (1-\alpha)\ m\ (r_{\mathrm{In}} + r_{\mathrm{Out}})$
State transition Active to Inactive	$7^3\ (\omega_w + 6\omega_c)\ \alpha\ m\ (r_{\mathrm{In}} + r_{\mathrm{Out}})$
IGMP membership queries/responses (soft)	$7^3\ \omega_c\ (\alpha m + 1)\ r_{\mathrm{MQR}}$
IGMP membership queries/responses (pred.)	$7^3\ \omega_c\ (\alpha m + \alpha m S_{\mathrm{MEPGr}} + S_{\mathrm{MEPGr}} + 1)\ r_{\mathrm{MQR}}$
PIM state refreshes	$(7^2 + 7^1)\ \omega_c\ r_{\mathrm{PIMR}}$
PIM hello messages	$(7^2 + 7^1)\ \omega_c\ r_{\mathrm{PIMH}}$
Handover signaling (soft)	$2\ 7^3\ (\omega_w + \omega_c)\ \alpha\ m\ r_{\mathrm{cc}}$
Handover signaling (pred.)	$2\ 7^3\ (\omega_w + 3\omega_c)\ \alpha\ m\ r_{\mathrm{cc}}$

Table C.3.: MB-ASM, MB-SSM: Analytical results of the signaling costs with paging support

C.4. Signaling Costs for the Case Study MB-CMAP

C.4.1. Signaling Costs Without Paging

The signaling costs specific to the case study MB-CMAP are caused by the handover signaling only. Unlike the case study MB-ASM, the signaling costs for inter-MEP advertisements[2] and for multicast signaling (membership queries/responses and PIM state refreshes) do not occur.[3]

The costs for handover signaling are comprised of signaling on the wireless link ($7^3\ \omega_w\ m\ r_{\mathrm{cc}}$), same as the case study MB-ASM) and on the wired links. The signaling costs on the wired links are (Fig. A.4(a), A.4(b), and A.5):

- For a hard and soft handover 10 signaling messages are generated (*Trace_Call Request* and *Response*, *Change_Owner Request*, *Response* and *Announce Change_Owner*, *Add_Ep Request*, *Response*, *Drop_Ep Request*, *Response*, *Announce Drop_Ep*). This results in signaling costs of ($10\ 7^3\ \omega_c\ m\ r_{cc}$), whereas the factor (10 represents the number of messages that is multiplied with the number of handover operations in the network ($7^3\ \omega_c\ m$) represents the weighted hop signaling messages generated in the network and r_{cc} the rate these messages are generated per mobile host.

- For the predictive handover it was assumed that for re-arranging the MEP group of a mobile host six operations are required (three MEPs are added and three are dropped to/from the multicast group). In this case, 20 signaling messages are generated (*Trace_Call Request* and *Response*, *Change_Owner Request*, *Response* and *Announce Change_Owner*, 3 *Add_Ep Request*,

[2] Due to the usage of third party signaling.

[3] Due to the usage hard multicast states that do not require state refreshes.

3 *Response*, 3 *Drop_Ep Request*, 3 *Response*, 3 *Announce Drop_Ep*). Then the signaling costs are ($20\ 7^3\ \omega_c\ m\ r_{cc}$).

The overall signaling costs are comprised of the components listed in Tab. C.4.

	Expression
MEP advertisements	$7^3\ \omega_w\ r_{\text{Adv}}$
Re-registrations	$2\ 7^3\ \omega_w\ m\ r_{\text{Rereg}}$
Handover signaling (hard and soft)	$7^3\ (2\omega_w + 10\omega_c)\ m\ r_{cc}$
Handover signaling (pred.)	$7^3\ (2\omega_w + 20\omega_c)\ m\ r_{cc}$

Table C.4.: MB-CMAP: Analytical results of the signaling costs without paging support

C.4.2. Signaling Costs With Paging

The support of inactive mobile hosts and paging causes the following signaling costs:

- *Paging_Update* and *Paging_Request* messages result in the same signaling costs as the case studies MB-ASM and MB-SSM: ($7^3\ (\omega_w + 3\omega_c)\ (1-\alpha)\ m\ r_{\text{PU}}$) for *Paging_Update* messages and ($7^3\ (2\omega_c + s_{\text{PA}}\omega_c + s_{\text{PA}}\omega_w)\ (1-\alpha)\ m\ r_{\text{In}}$) for *Paging_Request* messages.
- The state transition of a mobile host from the *inactive* to the *active* state (Fig. A.6(b)) results in a registration message from the mobile host to the access point and a *Open_Call* operation by the access point in order to create the multicast group and add their members. The *Open_Call* operation consists of a *Open_Call Request* and *Response* message and triggers implicitly an *Invite_Add_Ep Request* and *Response* message for each additional member of the multicast group. At all, for hard and soft handover 4 messages are generated (*Open_Call Request* and *Response*, *Invite_Add_Ep Request* and *Response*), whereas the *Open_Call Request* and *Response* messages are sent over a single wired link and the *Invite_Add_Ep Request* and *Response* message are sent over two wired links. For predictive handover ($2 + 2S_{\text{MEPGr}}$) messages are needed (*Open_Call Request* and *Response*, S_{MEPGr} x *Invite_Add_Ep Request* and *Response* to add all access points of the access point group to the call). Again, the *Open_Call Request* and *Response* messages are sent over a single wired link and the *Invite_Add_Ep Request* and *Response* messages are sent over 3 wired links. Then, the signaling costs for hard and soft handover amount to ($7^3\ (2\omega_w + 6\omega_c)\ (1-\alpha)\ m\ (r_{\text{In}} + r_{\text{Out}})$), and for predictive handover to ($7^3\ (2\omega_w + 2\omega_c + 2S_{\text{MEPGr}}\omega_c)\ (1-\alpha)\ m\ (r_{\text{In}} + r_{\text{Out}})$).
- The state transition of a mobile host from the *active* to the *inactive* state results in a registration message from the mobile host to the access point that in turn triggers a *Paging_Update* message to the gateway and a *Close_Call* operation. The latter *Close_Call* operation consists of a *Close_Call Request* and *Response* message and *Announce_Close_Call* messages to the other members of the multicast group (for hard and soft handover: 2 messages over 3 wired links and 1 message over 1 wired link (*Close_Call Request* and *Response* message and *Announce_Close_Call* message); for predictive handover: 2 messages over 3 three links (*Close_Call Request* and *Response* messages) and (S_{MEPGr}) messages over 1 link (*Announce_Close_Call* messages). The signaling costs amount to ($7^3\ (2\omega_w + 10\omega_c)\ \alpha\ m\ (r_{\text{In}} + r_{\text{Out}})$) for hard and soft handover and ($7^3\ (2\omega_w + 9\omega_c + S_{\text{MEPGr}}\omega_c)\ \alpha\ m\ (r_{\text{In}} + r_{\text{Out}})$) for predictive handover.

The resulting signaling costs are listed in Tab. C.5.

	Expression
MEP advertisements	$7^3\ \omega_w\ r_{\text{Adv}}$
Re-registrations of active mobile hosts	$2\ 7^3\ \omega_w\ \alpha\ m\ r_{\text{Rereg}}$
Paging updates of inactive mobile hosts	$7^3\ (\omega_w + 3\omega_c)\ (1-\alpha)\ m\ r_{\text{PU}}$
Paging requests	$7^3\ (s_{\text{PA}}\omega_w + 2\omega_c + s_{\text{PA}}\omega_c)\ (1-\alpha)\ m\ r_{\text{In}}$
State transitions Inactive-Active (hard, soft)	$7^3\ (2\omega_w + 6\omega_c)\ (1-\alpha)\ m\ (r_{\text{In}} + r_{\text{Out}})$
State transitions Inactive-Active (pred.)	$7^3\ (2\omega_w + 2\omega_c + 2\ S_{\text{MEPGr}}\omega_c)\ (1-\alpha)\ m\ (r_{\text{In}} + r_{\text{Out}})$
State transitions Active-Inactive (hard, soft)	$7^3\ (\omega_w + 10\omega_c)\ \alpha\ m\ (r_{\text{In}} + r_{\text{Out}})$
State transitions Active-Inactive (pred.)	$7^3\ (\omega_w + 2\omega_c + S_{\text{MEPGr}}\omega_c)\ \alpha\ m\ (r_{\text{In}} + r_{\text{Out}})$
Handover signaling (hard, soft)	$7^3\ (2\omega_c + 10\omega_c)\ \alpha\ m\ r_{cc}$
Handover signaling (pred.)	$7^3\ (2\omega_w + 20\omega_c)\ \alpha\ m\ r_{cc}$

Table C.5.: MB-CMAP: Analytical results of the signaling costs with paging support

C.5. Signaling Costs for the Case Study MIP-SGM

C.5.1. Signaling Costs Without Paging

The signaling costs for the case study MIP-SGM are comprised of the same components as the reference case basic and hierarchical Mobile IP: i) advertisements sent by foreign agents on the wireless link , ii) re-registrations, and iii) handover signaling. The first two components can be calculated by the same expressions as derived for Mobile IP in Sect. C.2. The third component is specific to the case study MIP-SGM.

The signaling costs for handover are caused by two signaling operations: The first creates the simultaneous binding in the switching foreign agent and home agent, respectively, by means of two messages (*Binding_Update Request* and *Response*). The second releases the simultaneous binding (also two messages). For SGM-enhanced basic Mobile IP the signaling messages are sent to the home agent. Since this analysis incorporates only signaling costs within the access network, 4 hops (one wireless and three wired hops) are considered. The signaling costs amount to $(4\ 7^3\ (\omega_w + 3\ \omega_c)\ m\ r_{cc})$. For SGM-enhanced hierarchical Mobile IP the signaling messages are sent to the switching foreign agent that is assumed to be at the first hierarchical level. Then, the signaling costs amount to $(4\ 7^3\ (\omega_w + \omega_c)\ m\ r_{cc})$.

The signaling costs are comprised of the components listed in Tab. C.6.

C.5.2. Signaling Costs With Paging

The support of inactive mobile hosts and paging results in additional signaling costs for *Paging_Update* and *Paging_Request* messages. The other signaling costs are decreased by the factor α since these operations pertain to the active mobile hosts only.

The signaling costs for *Paging_Update* and *Paging_Request* messages can directly be taken from the calculations of the other case studies.

	Expression
Foreign agent advertisements	$7^3\ \omega_w\ r_{\text{Adv}}$
Re-registrations	$2\ 7^3\ (\omega_w + 3\omega_c)\ m\ r_{\text{Rereg}}$
Handover signaling (Soft, SGM-enhanced basic Mobile IP)	$4\ 7^3\ (\omega_w + 3\omega_c)\ m\ r_{cc}$
Handover signaling (Soft, SGM-enhanced hierarchical Mobile IP)	$4\ 7^3\ (\omega_w + \omega_c)\ m\ r_{cc}$

Table C.6.: MIP-SGM: Analytical results of the signaling costs without paging support

State transitions of inactive mobile hosts to the active state cause a registration with signaling costs of $(7^3\ (2\omega_w + 6\omega_c)\ (1-\alpha)\ m\ (r_{\text{In}} + r_{\text{Out}}))$. State transitions of active mobile hosts becoming inactive generate signaling costs of $(7^3\ (2\omega_w + 6\omega_c)\ \alpha\ m\ (r_{\text{In}} + r_{\text{Out}}))$

The particular signaling costs are listed in Tab. C.7.

	Expression
Foreign agent advertisements	$7^3\ \omega_w\ r_{\text{Adv}}$
Re-registrations of active mobile hosts	$2\ 7^3\ (\omega_w + 3\omega_c)\ \alpha\ m\ r_{\text{Rereg}}$
Paging updates of inactive mobile hosts	$7^3\ (\omega_w + 3\omega_c)\ (1-\alpha)\ m\ r_{\text{PU}}$
Paging requests	$(7^3\ (s_{\text{PA}}\omega_w + 2\omega_c + s_{\text{PA}}\omega_c)\ (1-\alpha)\ m\ r_{\text{In}}$
State transitions Inactive-Active	$2\ 7^3\ (\omega_w + 3\omega_c)\ (1-\alpha)\ m\ (r_{\text{In}} + r_{\text{Out}})$
State transitions Active-Inactive	$2\ 7^3\ (\omega_w + \omega_c)\ \alpha\ m\ (r_{\text{In}} + r_{\text{Out}})$
Handover signaling (Soft, SGM-enhanced basic Mobile IP)	$4\ 7^3\ (\omega_w + 3\omega_c)\ \alpha\ m\ r_{cc}$
Handover signaling (Soft, SGM-enhanced hierarchical Mobile IP)	$4\ 7^3\ (\omega_w + \omega_c)\ \alpha\ m\ r_{cc}$

Table C.7.: MIP-SGM: Analytical results of the signaling costs with paging support

C.6. Numerical Results

In order to calculate the signaling costs, the variables are set to the values listed in Tab. C.8.

Fig. C.1 shows the signaling costs without paging. The variable m was varied from 0 to 30 mobile hosts per cell. This was achieved by changing the parameter δ from 0 to 0.1 ${}^{\text{mobile hosts}}/m^2$, whereas it is not distinguished between active and inactive mobile hosts. All other variables remained constant as listed in Tab. C.8. It can be seen that the signaling costs of all case studies is larger than the signaling costs of the reference case basic and hierarchical Mobile IP – except for the case study MB-ASM with soft handover where the signaling costs are similar to basic Mobile IP. In detail, the signaling costs of MB-ASM soft handover are 10–15 % higher than for hierarchical Mobile IP; the signaling costs of MB-ASM predictive handover up to 40 % (Fig. C.1(a)). The signaling costs of

Notation	Value	Notation	Value
ω_w	5	r_{Adv}	1/s
ω_c	1	$r_{IMEPAdv}$	0.2 /s
R	10 m	r_{MQR}	0.00833/s]
v	1 m/s	r_{PIMR}	0.01666/s
η	1	r_{PIMH}	0.03333/s
L	50 byte	r_{Rereg}	0.1/s
S_{MEPGr}	6 cells	r_{In}	0.001666 /s
s_{PA}	2	r_{Out}	0.001666 s

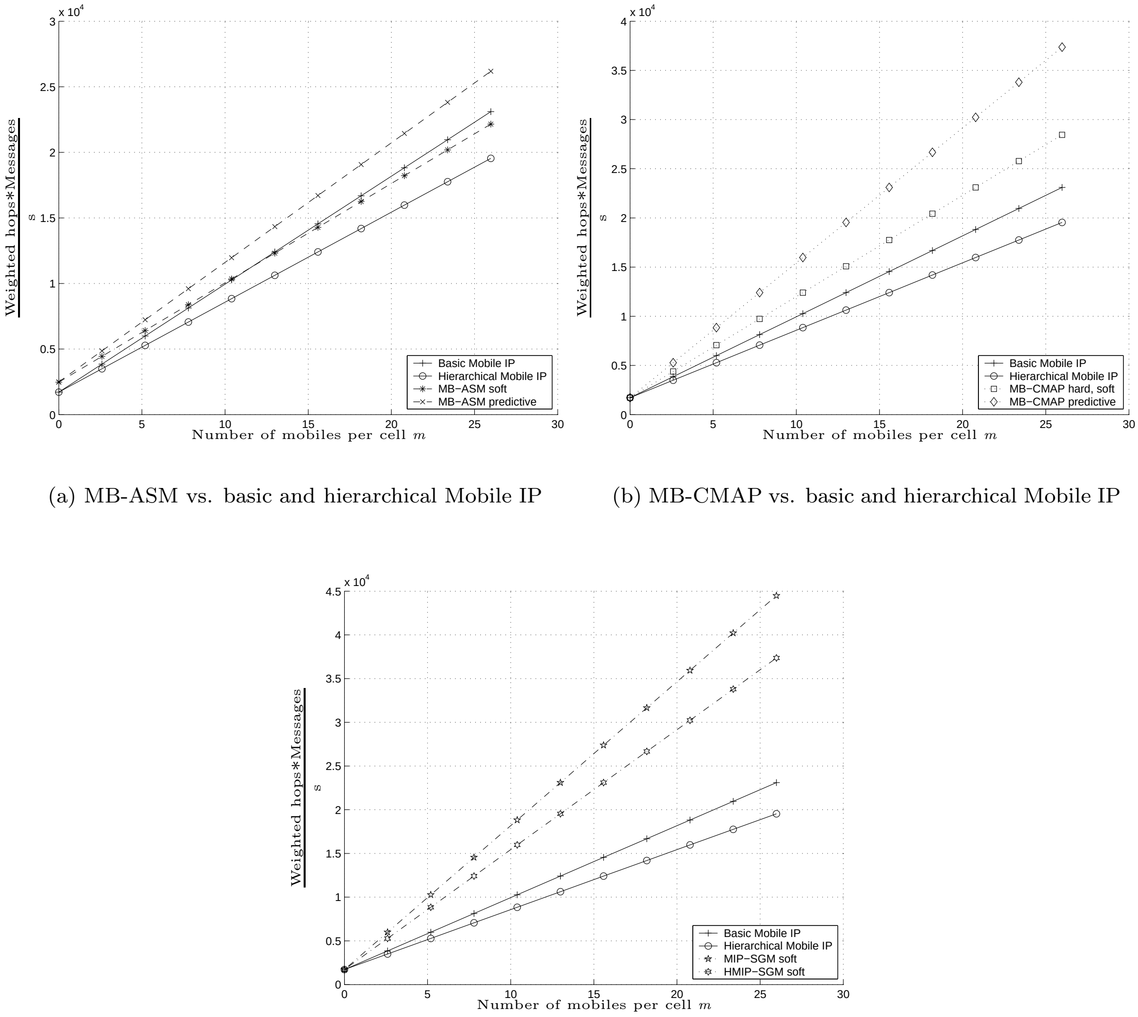
Table C.8.: Variable settings in the analytical evaluation of the signaling costs

MB-CMAP soft handover in comparison with hierarchical Mobile IP are up to 15 % higher; the signaling costs of MB-CMAP predictive handover of up to 90 % (Fig. C.1(b)). The case MIP-SGM causes signaling costs almost twice of the reference case: The signaling costs of SGM-enhanced basic Mobile IP is nearly twice of basic Mobile IP. The signaling costs of SGM-enhanced hierarchical Mobile IP is nearly twice of the reference case hierarchical Mobile IP.

Fig. C.2 demonstrates the benefits of supporting inactive mobile hosts and paging: The number of mobile hosts per cell m was set to the same values as before, but it was assumed that the proportion of active mobile hosts to the overall number of mobile hosts α is 1/2. The signaling costs of the case study MB-ASM for both soft and predictive handover are almost smaller than those of basic and hierarchical Mobile IP (for more than 3 mobile hosts per cell) (Fig. C.2(a)). The signaling costs of the case study MB-CMAP for all handover types becomes smaller than those of basic Mobile IP (Fig. C.2(b)). Also, the signaling costs of the case study MIP-SGM approximate to the costs of the reference cases.

In order to estimate the impact of the factor α on the signaling costs, the factor was varied from 0 to 1 whereas the δ was fixed to 0.1 resulting in 30 mobile hosts per cell ($m = 30$). In general, the point of intersection between the curves of signaling costs with paging and the signaling costs of the reference case basic and hierarchical Mobile IP gives a certain break even point for the proportion of active mobile hosts to the overall number α. Values of α lower than this break even point mean that the support of inactive mobile hosts and paging results in less signaling costs than the reference case.

Considering predictive handover — that causes higher signaling costs than soft handover – the break-even point is at $\alpha = 0.83$ for basic Mobile IP and $\alpha = 0.65$ for hierarchical Mobile IP (Fig. C.2(a)). For MB-CMAP predictive handover, the break-even point lies at $\alpha = 0.55$ for basic Mobile IP and at $\alpha = 0.42$ for hierarchical Mobile IP (Fig. C.2(b)). For the case study MIP-SGM with soft handover, the break-even point is reached at $\alpha = 0.42$ for SGM-enhanced basic Mobile IP compared with the reference case basic Mobile IP (and also for SGM-enhanced hierarchical Mobile IP compared with the reference case hierarchical Mobile IP).

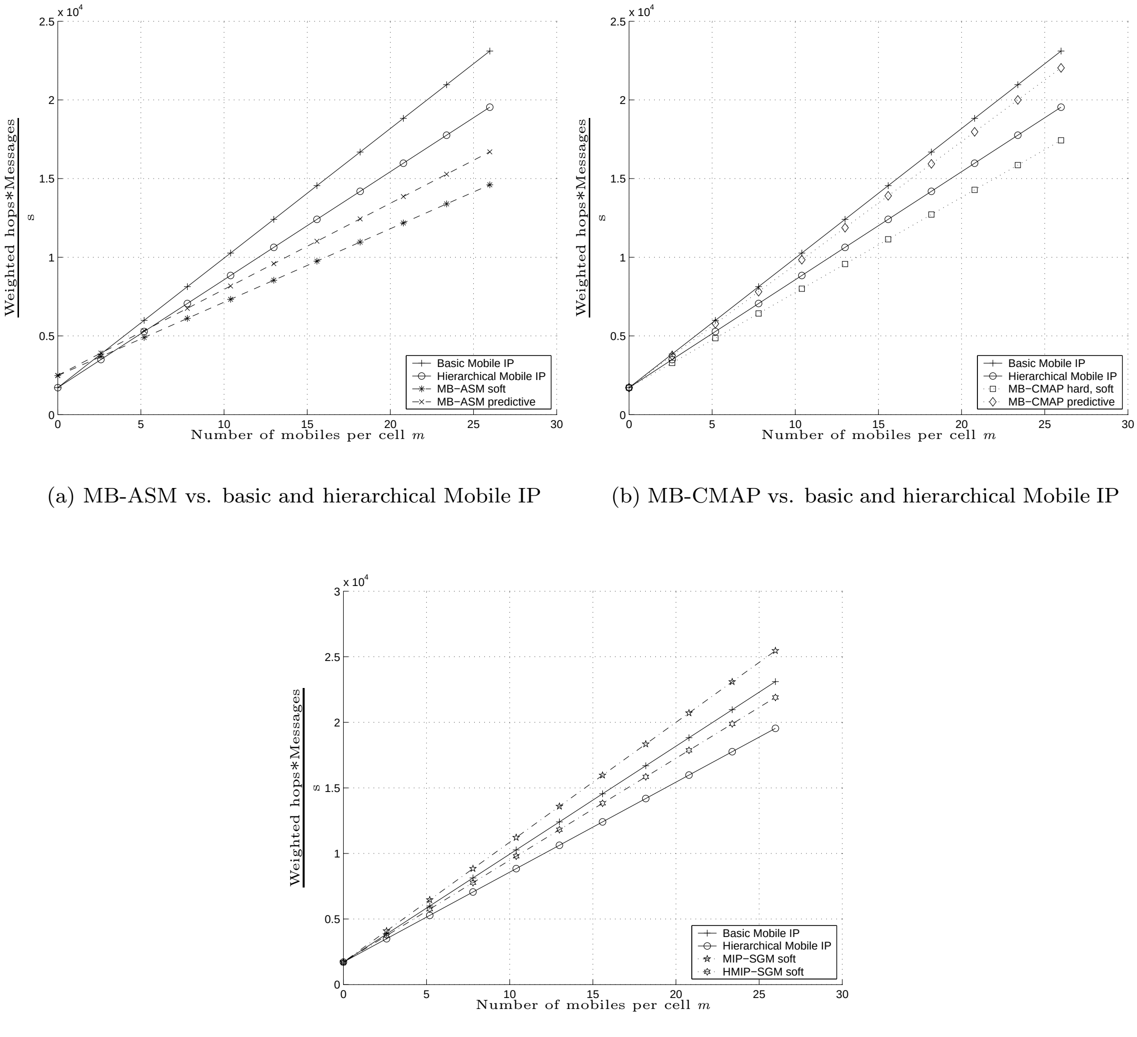


(a) MB-ASM vs. basic and hierarchical Mobile IP

(b) MB-CMAP vs. basic and hierarchical Mobile IP

(c) MIP-SGM vs. basic and hierarchical Mobile IP

Figure C.1.: Signaling costs without paging vs. number of mobiles per cell

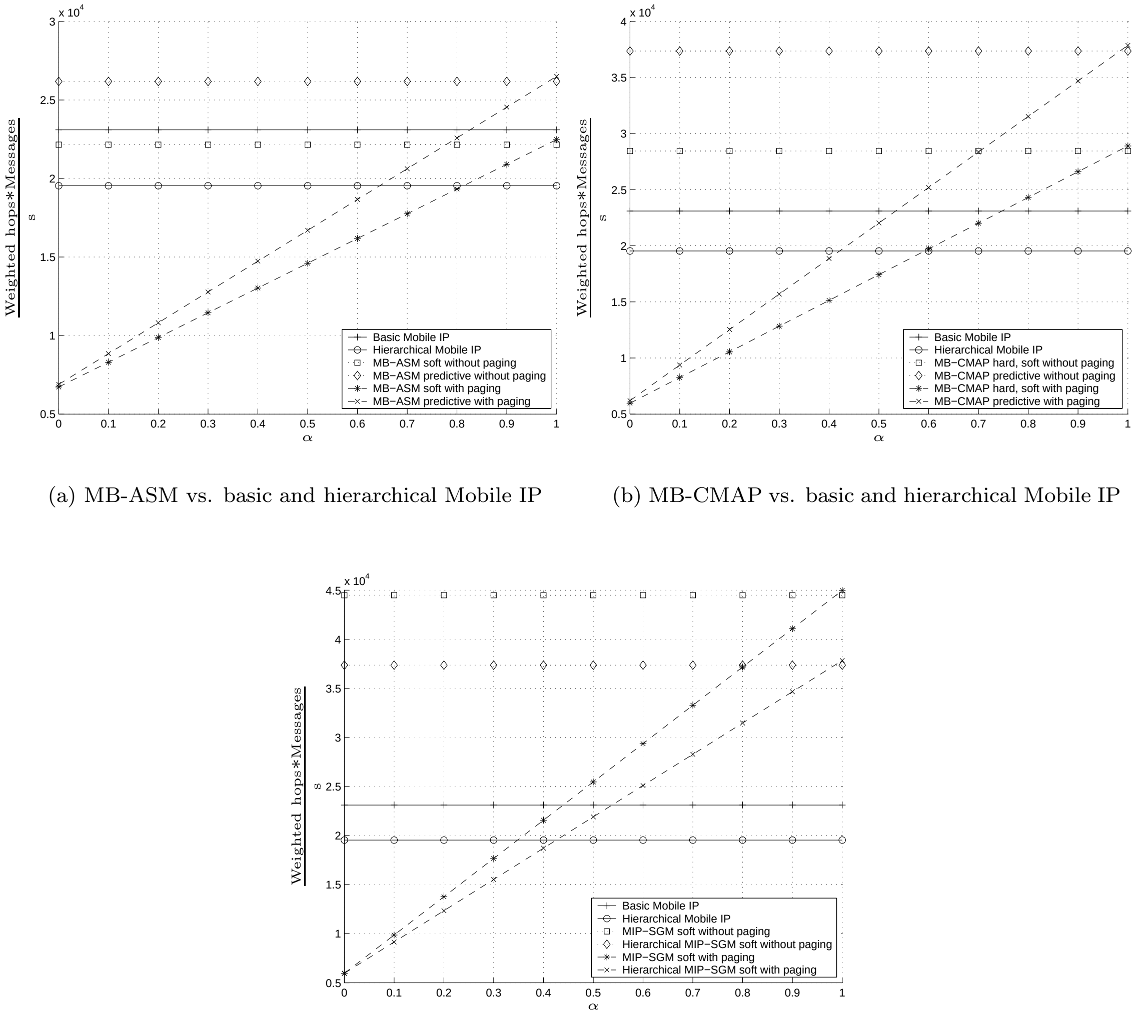


(a) MB-ASM vs. basic and hierarchical Mobile IP

(b) MB-CMAP vs. basic and hierarchical Mobile IP

(c) MIP-SGM vs. basic and hierarchical Mobile IP

Figure C.2.: Signaling costs with paging vs. number of mobiles per cell



(a) MB-ASM vs. basic and hierarchical Mobile IP

(b) MB-CMAP vs. basic and hierarchical Mobile IP

(c) MIP-SGM vs. basic and hierarchical Mobile IP

Figure C.3.: Signaling costs with paging vs. proportion of active mobile hosts to the overall number of mobile hosts

D. Acronyms

AAL ATM Adaption Layer

AI Advertisement Interval

AP Access Point

APIC ATM Port Interconnect Controller

ARP Address Resolution Protocol

AS Autonomous System

ASA Application Specific Address

ASM Any Source Multicast

ATM Asynchronous Transfer Mode

BGP Border Gateway Protocol

BUS Broadcast and Unknown Server

CBT Core Based Tree

CDT Cell Dwell Time

CH Correspondent Host

CIDR Classless Inter Domain Routing

CIMS Columbia University Micro-Mobility Suite

CLIP Classical IP over ATM

CMAP Connection Management Access Protocol

CMAP CM CMAP Connection Manager

CMAP SM CMAP Session Manager

CMNP Connection Management Network Protocol

CoA Care of Address

CSMA/CD Carrier Sense Multiple Access/Collsion Detection

DVMRP Distance Vector Multicast Routing Protocol

EARTH Easy IP Multicast Routing Through ATM Clouds

ECMP Express Count Management Protocol

ECS Eager Cell Switching

EFSM Extended Finite State Machine

EGP Exterior Gateway Protocol

ELAN Emulated LAN

EXPRESS EXplicitly Requested Single Source Multicast

FA Foreign Agent

FEC Forward Error Correction

FIFO First In First Out

GARP Generic Attribute Registration Protocol

GBNSC Gigabit Switch Controller

GMRP GARP Multicast Registration Protocol

GPL GNU General Public License

GPRS General Packet Radio Service

GSM Global System for Mobile Communciation

GW Gateway

GWP Gateway Proxy

HA Home Agent

HAWAII Handoff Aware Wireless Access Internet Infrastructure

HFA Highest Foreign Agent

HMIP Hierarchical Mobile IP

HVMP Host View Membership Protocol

IAP Iceberg Access Point

IAPP Inter Access Point Protocol

IC Integrated Circuit

ICEBERG Internet Core Beyond the Third Generation

ICQ I Seek You

IGMP Internet Group Management Protocol

IGP Interior Gateway Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IP Internet Protocol

IPv4 Internet Protocol Version 4

IPv6 Internet Protocol Version 6

ISO International Organization for Standardization

IS-95 Interim Standard for U.S. Code Division Multiple Access

LAN Local Area Network

LANE LAN Emulation

LB Lower Bound

LCS Lazy Cell Switching

LEO Low Earth Orbit

LFA Lowest Foreign Agent

LIS Logical IP Subnetwork

LL Link Layer

MAAA Multicast Address Allocation Architecture

MAC Medium Access Control

MARS Multicast Address Resolution Server

MBGP Multicast Border Gateway Protocol

MBone Multicast Backbone

MC Multicast

MCall Multi-Point Multi-Connection Call

MCN Multicast Node

MCS Multicast Server

MEP Mobility Enabling Proxy

MH Mobile Host

MIP Mobile IP

MLD Multicast Listener Discovery

MOMBASA Mobility Support - A Multicast Based Approach

MOMBASA SE MOMBASA Software Environment

MOSPF Multicast Extensions to Open Shortest Path First

MPA Mobile People Architecture

MS Microsoft

MSA Mobility Supporting Agent

MSDP Multicast Source Discovery Protocol

NA Not Applicable

NAT Network Address Translation

NIC Network Interface Card

NP Nondeterminstic Polynomial Time

ns network simulator

NWL Network Layer

OSI Open System Interconnection

PAT Personal Activity Tracker

PC Paging Cache

PDF Probability Distribution Function

PEP Performance Enhancing Proxy

PSTN Public Switched Telephone Network

PIM-DM Protocol Independent Multicast - Dense Mode

PIM-SM Protocol Independent Multicast - Sparse Mode

PIM-SSM Protocol Independent Multicast - Single Source Mode

PNNI Private Network Network Interface

PVC Permanent Virtual Circuit

QoS Quality of Service

RAT Reverse Address Translation

RC Routing Cache

RMTP Reliable Multicast Transport Protocol

RP Rendezvous Point

RPF Reverse Path Forwarding

RTP Real Time Protocol

RTT Round Trip Time

ReSoA Remote Socket Architecture

SAR Segmentation And Reassembling

SDL Specification and Description Language

SMDS Switched Multi-Megabit Data Service

SGM Small Group Multicast

SIP Session Invitation Protocol

SMS Selective Multicast Server

SNMP Simple Network Management Protocol

SSM Single Source Multicast

SPT Shortest Path Tree

SVC Switched Virtual Circuit

TCP Transmission Control Protocol

TDMA Time Division Multiple Access

TTL Time To Live

UB Upper Bound

UC Unicast

UDP User Datagram Protocol

UML Unified Modeling Language

UMTS Universal Mobile Telecommuniation System

UNI User Network Interface

URL Universal Ressource Locator

UTOPIA Universal Test and Operations Physical Interface for ATM

UTRAN Universal Terrestrial Radio Access Network

VC Virtual Circuit

VENUS Very Extensive Non-Unicast Service

WAN Wide Area Network

WB-CDMA Wideband Code Division Multiple Access

WDM Wavelength Division Multiplexing

WUGS Washington University Gigabit Switch

WLAN Wireless Local Area Network

XCast Explicit Multicast

Bibliography

[1] A. Acampora and M. Naghshineh. An Architecture and Methodology for Mobile-Executed Handoff in Cellular ATM Networks. *IEEE Journal on Selected Areas in Communication*, 12 (8):1365–1375, 1994.

[2] A. Acharya and B. Badrinath. A Framework for Delivering Multicast Messages in Networks With Mobile Hosts. *ACM/Baltzer Journal of Mobile Networks and Applications (MONET)*, 1(2):199–219, 1996.

[3] A. Adams, J. Nicholas, and W. Siadak. Protocol Independent Multicast - Dense Mode (PIM-DM) Protocol Specification (Revised). Internet Draft (Work in progess), October 2003.

[4] L. Aguilar. Datagram Routing For Internet Multicasting. In *Proceedings ACM SIGCOMM'84 Communications Architectures and Protocols*, pages 58–63, Montreal, Quebec, Cananda, June 1984.

[5] K. Almeroth. The Evolution of Multicast: From the MBone to Inter-Domain Multicast to Internet2 Deployment. *IEEE Network*, 14(1):10–20, 2000.

[6] W. Almesberger. ATM on Linux. `http://linux-atm.sourceforge.net/`.

[7] G. Appenzeller, K. Lai, P. Maniatis, M. Roussopoulos, E. Swierk, X. Zhao, and M. Baker. The Mobile People Architecture. Technical Report CSL-TR-99-777, Stanford University, Junuary 1999.

[8] G. Armitage. IP Multicasting Over ATM Networks. *IEEE Journal on Selected Areas in Communication*, 15(32):445–457, 1997.

[9] G. Armitage. VENUS - Very Extensive Non-Unicast Service. Internet RFC 2191, September 1997.

[10] A. Ballardie. Core Based Trees (CBT) Multicast Routing Architecture. Internet RFC 2201, September 1997.

[11] A. Ballardie. Core Based Trees (CBT Version 2) Multicast Routing Architecture – Protocol Specification. Internet RFC 2189, September 1997.

[12] R. Ballardie, R. Perlman, C. Lee, and J. Crowcroft. Simple Scalable Internet Multicast. Technical Report UCL Research Note RN/99/21, University College London (UCL), April 1999.

[13] T. Bates, R. Chandra, D. Katz, and Y. Rekhter. Multiprotocol Extensions for BGP-4. Internet RFC 2283, February 1998.

[14] J. Belopilski. Implementierung und Test von Policies fuer Multicast-Basierten Handover in einem Experimentellen Testbett. Studienarbeit, TKN, TU Berlin, November 2001.

[15] C. Bettstetter. Smooth is Better Than Sharp: A Random Mobility Model for Simulation of Wireless Networks. In *Proceedings of ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'01)*, pages 19–27, Rome, Italy, July 2001.

[16] S. Bhattacharyya, C. Diot, L. Giuliano, R. Rockell, J. Meylor, D. Meyer, G. Shepherd, and B. Haberman. An Overview of Source-Specific Multicast(SSM) Deployment. Internet Draft (Work in progess), November 2002.

[17] U. Black. *Voice Over IP*. Series in Advanced Communications Technologies. Prentice Hall, 2nd ed. edition, 2002. ISBN 0-13-065204-0.

[18] H. Boche and E. Jugl. Extension of ETSI's Mobility Models For UMTS In Order To Get More Realistic Results. In *Proceedings of UMTS Workshop*, Guenzburg, Germany, November 1998.

[19] R. Boivie. A New Multicast Scheme for Small Groups. Research Report RC21512(97046)29JUNI1999, IBM T. J. Watson Research Center, June 1999.

[20] R. Boivie and N. Feldman. Small Group Multicast. Internet Draft (Expired), July 2000.

[21] R. Boivie, N. Feldman, Y. Imai, W. Livens, D. Ooms, and O. Paridaens. Explicit Multicast (Xcast) Basic Specification. Internet Draft (Work in progress), July 2003.

[22] J. Border, J. Griner, G. Montenegro, and Z. Shelby. Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations. Internet RFC 3135, June 2001.

[23] E. Brewer, R. Katz, Y. Chawathe, T. Gribble, S. Hodes, G. Nguyen, M. Stemm, E. Henderson, T. Amir, H. Balakrishnan, A. Fox, V. Padmanabhan, and S. Seshan. A Network Architecture for Heterogeneous Mobile Computing. *IEEE Personal Communications Magazine*, 5(5):8–24, 1998.

[24] R. Caceres and V.N. Padmanabhan. Fast and Scalable Handoffs for Wireless Internetworks. In *Proceedings ACM MobiCom'96*, pages 55–66, Rye, NY, USA, November 1996.

[25] B. Cain, S. Deering, A. Denner, I. Kouvelas, and A. Thyagarajan. Internet Group Management Protocol, Version 3. Internet RFC 3376, October 2002.

[26] A. Campbell, W. Chieh-Yih, J. Gomez, S. Kim, and A. Valko. Columbia IP Micro-Mobility Software. `http://comet.ctr.columbia.edu/micromobility/`.

[27] A. Campell, J. Gomez, S. Kim, A. Valko, C.-Y. Wan, and Z. Turanyi. Design, Implementation, and Evaluation of Cellular IP. *IEEE Personal Communication*, pages 42–49, August 2000.

[28] T. Chaney, A. Fingerhut, M. Flucke, and J. Turner. Design of a Gigabit ATM Switch. In *Proceedings of IEEE Infocom'97*, pages 2–11, Kobe, Japan, April 1997.

[29] Y. Chawathe. *Scattercast: An Architecture for Internet Broadcast Distribution as an Infrastructure Service.* Dissertation, University of California at Berkeley, 2000.

[30] V. Chikarmane, C. Williamson, R. Bunt, and W. Mackrell. Multicast Support for Mobile Hosts Using Mobile IP: Design Issues and Proposed Architecture. *ACM/Baltzer Journal of Mobile Networks and Applications (MONET)*, 3(4):365–379, 1998.

[31] Y.-H. Chu, S. G. Rao, S. Sehshan, and Zhang.H. Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture. In *Proceedings on ACM SIGCOMM 2001 Conference: Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 55–67, San Diego, CA, USA, 2001.

[32] Y.-H. Chu, S. G. Rao, and Zhang.H. A Case for End System Multicast. In *Proceedings of ACM SIGMETRICS 2000*, pages 1–12, Santa Clara, CA, USA, June 2000.

[33] D. Cohen. Issues in Transnet Packetized Voice Communications. In *Proceedings of the Fifth IEEE Data Communications Symposium*, pages 6–13, Snowbird, UT, USA, September 1977.

[34] The ATM Forum Technical Commitee. LAN Emulation Client Management Specification Version 1.0. ATM Forum Specification, September 1995.

[35] The ATM Forum Technical Commitee. LAN Emulation Over ATM Version 1.0. ATM Forum Specification, January 1995.

[36] The ATM Forum Technical Commitee. LAN Emulation Server Management Specification Version 1.0. ATM Forum Specification, March 1996.

[37] The ATM Forum Technical Commitee. LAN Emulation over ATM Version 2 – LUNI Specification. ATM Forum Specification, July 1997.

[38] The ATM Forum Technical Commitee. LAN Emulation Client Management Specification Version 2.0. ATM Forum Specification, October 1998.

[39] Comprehensive Perl Archive Network. `http://www.cpan.org`.

[40] K. Cox and J. deHart. Connection Management Access Protocol (CMAP) Specification. Applied Research Laboratory Working Note ARL 94-21, Washington University, St. Louis, MO, USA, July 1994.

[41] E. Dahlmann, M. Gudmundsson, M. Nilsson, and J. Sköld. UMTS/IMT-2000 Based on Wideband CDMA. *IEEE Communications Magazin*, pages 70–80, September 1998.

[42] DARPA. Transmission Control Protocol. Internet RFC 793, September 1981.

[43] S. Deering, D. Estrin, D. Farinacci, M. Handley, A. Helmy, V. Jacobson, L. Wei, P. Sharma, and D. Thaler. Protocol Independent Multicast-Sparse Mode (PIM-SM): Motivation and Architecture. Internet Draft (Expired), October 1994.

[44] S. Deering, W. Fenner, and B. Haberman. Multicast Listener Discovery (MLD) for IPv6. Internet RFC 2710, October 1999.

[45] J. deHart. Connection Management Network Protocol (CMNP) Specification. Applied Research Laboratory Working Note ARL 94-14, Washington University, St. Louis, MO, USA, September 1994.

[46] C. Diot and L. Gautier. A Distributed Architecture for Multiplayer Interactive Applications on the Internet. *IEEE Network*, 13(4):6–15, 1999.

[47] C. Diot, B. Levine, B. Lyles, H. Kassem, and D. Balensiefen. Deployment Issues for the IP Multicast Service and Architecture. *IEEE Network*, 14(1):78–88, 2000.

[48] Z. Dittia, J. Cox, and G. Parulkar. Design of the APIC: A High Performance ATM Host-Network Interface Chip. In *Proceedings of IEEE Infocom '95*, pages 179–187, Boston, MA, USA, April 1995.

[49] R. Droms. Dynamic Host Configuration Protocol. Internet RFC 1541, October 1993.

[50] J. Ellsberger, D. Hogrefe, and A. Sarma. *SDL Formal Object-oriented Language for Communication Systems.* Prentice Hall, 1997. ISBN 0-13-621384.

[51] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, and L. Wei. Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification. Internet RFC 2362, June 1998.

[52] K. Fall and K. (Editors) Varadhan. The ns Manual (formerly ns Notes and Documentation). `http://www.isi.edu/nsnam/ns/doc-stable/index.html`, August 2000.

[53] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina. Generic Routing Encapsulation. Internet RFC 2784, March 2000.

[54] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised). Internet Draft (Work in progress), March 2001.

[55] W. Fenner. Internet Group Management Protocol, Version 2. Internet RFC 2236, November 1997.

[56] A. Festag. CMAP HOW TO - A Short Guide to Install, Configure and Start Up CMAP. Technical Report TKN-00-004, Telecommunication Networks Group, Technische Universität Berlin, June 2000.

[57] A. Festag. Optimization of Handover Performance by Link Layer Triggers in IP-Based Networks; Parameters, Protocol Extensions, and APIs for Implementation. Technical Report TKN-02-014, Telecommunication Networks Group, Technische Universität Berlin, July 2002.

[58] A. Festag, H. Karl, and A. Wolisz. Classification and Evaluation of Multicast-Based Mobility Support in All-IP Cellular Networks. In *Proceedings of Kommunikation in Verteilten Systemen (KiVS 2003)*, Leipzig, Germany, February 2003.

[59] A. Festag and L. Westerhoff. Protocol Specification of the MOMBASA Software Environment. Technical Report TKN-01-014, TKN, TU Berlin, Berlin, Germany, May 2001.

[60] A. Festag, L. Westerhoff, and A. Wolisz. The MOMBASA Software Environment – A Toolkit for Performance Evaluation of Multicast-Based Mobility Support. In *Proceedings of Performance Tools 2002*, pages 212–219, London, GB, April 2002.

[61] American National Standard for Telecommunications. American National Standard for Telecommunications - Digital Hierarchy - Optical Interface Rates and Formats Specification,. ANSI T1.105-20011, 2001.

[62] D. Forsberg, J. T. Malinen, J. K. Malinen, and H. H. Kari. Increasing Communication Availability With Signal-Based Mobile Controlled Handoffs. In *Proceedings of IP based Cellular Networks (IPCN2000)*, Paris, France, May 2000.

[63] D. Forsberg, J. T. Malinen, T. Weckstroem, and M. Tiusanen. Distributing Mobility Agents Hierarchically under Frequent Location Update. In *Proceedings of Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99)*, pages 159–168, San Diego, CA, USA, 1999.

[64] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. Internet RFC 1467, September 1993.

[65] M.E. Gaddis, R. Bubenik, and J. Dehart. A Call Model for Multipoint Communication in Switched Networks. In *Proceedings of IEEE International Conference on Communications, Supercomm/ICC '92*, pages 609–615, 14-18 1992.

[66] R. Ghai and S. Singh. An Architecture and Communication Protocol for Picocellular Networks. *IEEE Personal Communications Magazine*, 1(3):36–46, 1994.

[67] D. Ginsburg. *ATM Solutions For Enterprise Networking*. Data Communications and Networks Series. Addison Welsey Longman Limited, 1996. ISBN 0-201-34302-9.

[68] GNU's not Unix. `http://www.gnu.org`.

[69] GNU General Public License. `http://www.gnu.org/copyleft/gpl.html`.

[70] E. Gustavsson, A. Jonsson, and C. Perkins. Mobile IPv4 Regional Registration. Internet Draft, October 2002.

[71] J. Haartsen, M. Naghshineh, J. Inouye, O. Joeressen, and W. Allen. Bluetooth: Vision, Goals, and Architecture. *Mobile Computing and Communications Review*, 2(4):38–45, 1998.

[72] B. Haberman. Dynamic Allocation Guidelines for IPv6 Multicast Addresses. Internet Draft work in progess, October 2001.

[73] F. Halsall. *Data Communications, Computer Networks and Open Systems*. Addison-Wesley, 1996. ISBN 0-201-42293.

[74] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberger. SIP: Session Initiation Protocol. Internet RFC 2543, May 1999.

[75] H. Hartenstein, K. Jonas, and R. Schmitz. Seamless Inter-Domain Handoffs via Simultaneous Bindings. In *Proceedings of European Wireless 2000 together with ECRR'2000*, Dresden, Germany, September 2000.

[76] D. Helder and S. Jamin. Banana Tree Protocol, an End-host Multicast Protocol. Technical Report CSE-TR-429-00, University of Michigan, 2000.

[77] A. Helmy. Multicast-based Architecture for IP Mobility: Simulation Analysis and Comparison with Basic Mobile IP. Technical Report USC-CS-TR-00-734, Electrical Engineering Department, University of Southern California, June 2000.

[78] A. Helmy. A Multicast-based Protocol for IP Mobility Support. In *Proceedings of ACM Second International Workshop on Networked Group Communication (NGC 2000)*, pages 49–58, Palo Alto, CA, USA, November 2000.

[79] A. Helmy. State Analysis and Aggregation Study for Multicast-based Micro Mobility. In *Proceedings of IEEE International Conference on Communications (ICC 2002), Symposium on Wireless Networking Theory*, New York, USA, May 2002.

[80] H. Hersent, D. Gurle, and J.-P. Petit. *IP Telephony Packet-based Multimedia Communications Systems*. Pearson Education Limited, 2000. ISBN 0-201-61910-0.

[81] H. Holbrook and B. Cain. Source-Specific Multicast for IP. Internet Draft (Work in progess), November 2002.

[82] H. W. Holbrook and D. R. Cheriton. IP Multicast Channels: EXPRESS Support for Large-scale Single-source Applications. In *Proceedings of ACM SIGCOMM 1999*, pages 65–78, Cambridge, MA, USA, 1999.

[83] G. J. Holzmann. *Design and Validation of Computer Protocols*. Prentice Hall, 1991. ISBN 0-13539925-4.

[84] D. Hong and S. Rappaport. Traffic Model and Performance Analysis for Cellular Mobile Radio Telephone Systems with Prioritized and Nonprioritized Handoff Procedures. *IEEE Transactions on Vehicular Technology*, VT-35(3):77–92, 1986.

[85] G. Huston. Commentary on Inter-Domain Routing in the Internet. Internet RFC 3221, December 2001.

[86] IEEE Std 802.11, 1999 Edition. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[87] IEEE Std 802.11a, 1999 Edition. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 1: High-speed Physical Layer in the 5 GHz band.

[88] IEEE Std 802.11b, 1999 Edition. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band.

[89] IEEE Std 802.1B, 1995 Edition. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Common specifications – Part 2: LAN/MAN management.

[90] IEEE Std 802.3, 1996 Edition. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification.

[91] IEEE Std 802.4, 1990 Edition. Information processing systems – Local area networks – Part 4: Token-passing bus access method and physical layer specifications.

[92] IEEE Std 802.5, 1998 Edition. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 5: Token ring access method and physical layer specifications.

[93] R. Jain. *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. John Wiley and Sons, Inc., 1991. ISBN 0-471-50336-3.

[94] J. Jannotti, D. Gifford, K. Johnson, M. Kaashoek, and J. O'Toole. Overcast: Reliable Multicasting with an Overlay Network. In *Proceedings of the Fourth Symposium on Operating Systems Design and Implementation. USENIX Association*, pages 197–212, San Diego, CA, USA, 2000.

[95] A. Jimenez. Simulative of Multicast-Enhanced Mobile IP and Hierarchical Mobile IP. Diploma Thesis, TKN, TU Berlin, July 2002.

[96] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. Internet Draft (Work in progress), February 2003.

[97] K. Keeton, B. Mah, S. Seshan, R. Katz, and D. Ferrari. Providing Connection-Oriented Network Services to Mobile Hosts. In *Proceedings of the USENIX Symposium on Mobile and Location-Idependent Computing*, pages 83–102, Cambridge, MA, USA, August 1993.

[98] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. Internet RFC 2401, November 1998.

[99] S. Kumar, P. Radoslavov, D. Thaler, C. Alaettinoglu, D. Estrin, and M. Handley. The MASC/BGMP Architecture for Inter-Domain Multicast Routing. In *Proceedings of SIGCOMM 1998*, pages 93–104, Vancouver, BC, Canada, August 1998.

[100] J. Kurose and K. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet.* Addison Wesley Longman, Inc., 2001. ISBN 0-201-47711-4.

[101] M. Laubach. Classical IP and ARP over ATM. Internet RFC 1577, January 1994.

[102] E. M. Law and W. D. Kelton. *Simulation Modeling and Analysis.* Series in Industrial Engineering and Management Science. McGraw-Hill, 1992. ISBN 0-07-100803-9.

[103] Linux Operating System. `http://www.kernel.org`.

[104] G. Malkin. RIP Version 2. Internet RFC 2453, November 1998.

[105] P. Maniatis, M. Roussopoulos, E. Swierk, M. Lai, G. Appenzeller, X. Zhao, and M. Baker. The Mobile People Architecture. *ACM Mobile Computing and Communications Review (MC2R)*, July 1999.

[106] D. Meyer and B. Fenner. Multicast Source Discovery Protocol (MSDP). Internet Draft work in progess, November 2002.

[107] D. Meyer and P. Lothberg. GLOP Addressing in 233/8. Internet RFC 2770, February 2000.

[108] A. Mihailovic, M. Shabeer, and A. H. Aghvami. Sparse Mode Multicast as a Mobility Solution for Internet Campus Networks. In *Proceedings of the tenth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 1999 (PIMRC'99)*, Osaka, Japan, September 1999.

[109] A. Mihailovic, M. Shabeer, and A. H. Aghvami. Multicast For Mobility Protocol (MMP) For Emerging Internet Networks. In *Proceedings of the eleventh IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2000)*, London, UK, September 2000.

[110] H. Moeland and M. Trompower. Inter-Access Point Protocol Wireless Networking Distribution System Communication. Internet Draft (Expired), March 1998.

[111] J. Mogul and J. Postel. Internet Standard Subnetting Procedure. Internet RFC 950, August 1985.

[112] J. Moy. Multicast Extensions to OSPF. Internet RFC 1584, March 1994.

[113] J. Moy. OSPF Version 2. Internet RFC 2328, April 1998.

[114] M. Moyer, J. R. Rao, and P. Rohathi. A Survey of Security Issues in Multicast Communications. *IEEE Network*, 13(6):12–23, 1999.

[115] J. Mysore and V. Bharghavan. A New Multicast-Based Architecture for Internet Mobility. In *Proceedings of the Third ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'97)*, pages 161 – 172, Budapest, Hungary, October 1997.

[116] J. Mysore and B. Vaduvur. Performance of Transport Protocols Over a Multicasting-Based Architecture For Internet Host Mobility. In *Proceedings of International Conference on Communication (ICC'98)*, volume 3, pages 1817–1823, Piscataway, NJ, USA, 1998.

[117] NetPerf. `http://www.netperf.org/netperf/NetperfPage.html`.

[118] NET-SNMP. `http://www.net-snmp.org`.

[119] University of Southern California. Gigabit Network Technology Distribution Program. `http://www.arl.wustl.edu/gigabitkits`.

[120] University of Southern California. USC pimd PIM-SM Version 2 Multicast routing daemon. `http://catarina.usc.edu/pim/`, 2000.

[121] Helsinki University of Technology Dynamics Group. Dynamics - HUT Mobile IP. `http://www.cs.hut.fi/Research/Dynamics/`.

[122] T. Ojanpera and R. Prasad. *WCDMA: Towards IP Mobility and Mobile Internet*. Artech House Universal Personal Communication Series. Artech House Publisher, 2001. ISBN 1-58053-180-6.

[123] D. Ooms, W. Livens, and O. Paridaens. Connectionless Multicast. Internet Draft (Expired), April 2000.

[124] S. Ostermann. tcptrace. `http://jarok.cs.ohiou.edu/software/tcptrace/tcptrace.html`.

[125] Packet Capture Library. `ftp://ftp.ee.lbl.gov/libpcap.tar.Z`.

[126] S. Paul. *Multicasting on the Internet and its Applications*. Kluwer Academic Publisher, 1998. ISBN 0-7923-8200-5.

[127] S. Paul, K.K. Sabnani, J.C. Lin, and S. Bhattacharyya. Reliable Multicast Transport Protocol (RMTP). *IEEE Journal on Selected Areas in Communications*, 15(3):407–421, 1997.

[128] C. Perkins. IP Encapsulation within IP. Internet RFC 2003, October 1996.

[129] C. Perkins. IPv4 Mobility Support. Internet RFC 2002, October 1996.

[130] C. Perkins. Minimal Encapsulation within IP. Internet RFC 2004, October 1996.

[131] C. Perkins. *Mobile IP Design Principles and Practices*. Addison-Wesley Longman, Reading, MA, USA, 1998. ISBN 0-201-63469.

[132] J. Postel. User Datagram Protocol. Internet RFC 768, August 1980.

[133] R. Ramjee, J. Kurose, D. Towsley, and H. Schulzrinne. Adaptive Playout Mechanisms for Packetized Audio Applications in Wide-Area networks. In *Proceedings of IEEE Infocom '94*, pages 680–688, Toronto, Canada, June 1994.

[134] R. Ramjee and T. LaPorta. Paging Support for IP Mobility. Internet Draft (Exired), July 2000.

[135] R. Ramjee, T. LaPorta, S. Thuel, and K. Varadhan. IP Micro-Mobility Support Using HAWAII. Internet Draft (Expired), July 2000.

[136] R. Ramjee, T. LaPorta, S. Thuel, K. Varadhan, and S. Wang. HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks. In *Proceedings of ICNP'99*, Toronto,Canada, October/November 1999.

[137] Redhat Linux Distribution. `http://www.redhat.com`.

[138] Y. Rekhter and T. Li. An Architecture for IP Address Allocation with CIDR. Internet Internet RFC 1467, September 1993.

[139] Y. Rekhter and T. Li. A Border Gateway Protocol 4 (BGP-4). Internet RFC 1771, March 1995.

[140] M. Roussopoulos, P. Maniatis, E. Swierk, K. Lai, G. Appenzeller, and M. Baker. Person-Level Routing in the Mobile People Architecture. In *Proceedings of the USENIX Symposium on Internet Technologies and Systems*, October 1999.

[141] M. Schläger. Softlink. `http://www-tkn.ee.tu-berlin.de`.

[142] M. Schläger, B. Rathke, S. Bodenstein, and A. Wolisz. Advocating a Remote Socket Architecture for Internet Access using Wireless LANs. *ACM/Baltzer Mobile Networks and Applications (Special Issue on Wireless Internet and Intranet Access)*, 6(1):23–2, 2001.

[143] J. W. Schmidt and R. E. Taylor. *Simulation and Analysis of Industrial Systems*. Richard D. Irwin, Inc., Homewood, Illinois, USA, 1970.

[144] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. Internet RFC 1889, January 1996.

[145] S. Seshan. *Low-Latency Handoffs for Cellular Data Networks*. Ph.d. thesis, University of Berkeley at California, March 1996.

[146] T. J. Shepard. xplot. `http://www.xplot.org`.

[147] R. Singh, Y. C. Tay, W. T. Teo, and S. W. Yeow. RAT: A Quick (And Dirty?) Push for Mobility Support. In *Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications*, pages 32–40, New Orleans, LA, USA, February 1999.

[148] M. Smirnov. EARTH - Easy IP multicast routing THrough ATM clouds. Internet Draft (Expired), March 1997.

[149] P. Srisuresh and K. Egevang. Traditional IP Network Address Translator (Traditional NAT). Internet RFC 3022, January 2001.

[150] M. Stemm and R. Katz. Vertical Handoffs in Wireless Overlay Networks. *ACM Mobile Networking (MONET), Special Issue on Mobile Networking in the Internet*, Winter 1998.

[151] StrongARM processors. `http://www.arm.com/armtech/StrongARM`.

[152] SuSE Linux Distribution. `http://www.suse.de`.

[153] D. Thaler and M. Handley. On the Aggregatability of Multicast Forwarding State. In *Proceedings of IEEE Infocom 2000*, volume 3, pages 1654–1663, March 2000.

[154] D. Thaler, M. Handley, and D. Estrin. The Internet Multicast Address Allocation Architecture. Internet RFC 2908, September 2000.

[155] C. Topolcic. Status of CIDR Deployment in the Internet. Internet RFC 1467, August 1993.

[156] H. Uzunalioglu, I. Akyildiz, Y. Yesha, and E. Yen. Footprint Handover Rerouting Protocol for Low Earth Orbit Satellite Networks. *ACM Baltzer Journal of Wireless Networks (WINET)*, 5(5), 1999.

[157] A. Valko. Cellular IP - A New Approach to Internet Host Mobility. *ACM Computer Communication Review*, 29(1):50–65, 1999.

[158] M. Villén-Altamirano and J. Villén-Altamirano. RESTART: A Method for Accelerating Rare Event Simulations. In C. D. Pack, editor, *Queueing, Performance and Control in ATM*, pages 71–76. Elsevier Science Publishers B. V., June 1991.

[159] D. Waitzmann, C. Patridge, and S. Deering. Distance Vector Multicast Routing Protocol (DVMRP). Internet RFC 1075, November 1988.

[160] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner. The VersaKey Framework: Versatile Group Key Management. *IEEE Journal on Selected Areas in Communications*, 17 (8):1614–1631, 1999.

[161] H. J. Wang, B. Raman, C. Chuah, R. Biswas, R. Gummadi, B. Hohlt, X. Hong, E. Kiciman, Z. Mao, J. S. Shih, L. Subramanian, B.Y. Zhao, A. D. Joseph, and R. Katz. ICEBERG: An Internet-Core Network Architecture for Integrated Communications. *IEEE Personal Communications*, 7(4):10–19, 2000.

[162] E. Wedlund and H. Schulzrinne. Mobility Support Using SIP. In *Proceedings of Second ACM/IEEE International Conference on Wireless and Mobile Multimedia WoWMoM99*, pages 76–82, Seattle, WA, USA, August 1999.

[163] M. Weiser. The Computer for the 21st Century. *Scientific American*, 3(265):94–104, 1991.

[164] L. Westerhoff. Implementation of Multicast-Based Mobility Support and Setup of an Experimental Testbed. Diploma Thesis, TKN, TU Berlin, November 2001.

[165] L. Westerhoff and A. Festag. Implementation of the MOMBASA Software Environment. Download at `http://www-tkn.ee.tu-berlin.de/research/mombasa/mse.html`.

[166] L. Westerhoff and A. Festag. Implementation Design of the MOMBASA Software Environment. Technical Report TKN-01-017, TKN, TU Berlin, Berlin, Germany, November 2001.

[167] L. Westerhoff and A. Festag. Testing the Implementation of the MOMBASA Software Environment. Technical Report TKN-01-018, TKN, TU Berlin, Berlin, Germany, December 2001.

[168] J. Widmer. Network Simulations for a Mobile Network Architecture for Vehicles. Technical Report TR-00-009, Internation Comuter Science Institute (ISI), Berkeley, CA, USA, May 2000.

[169] R. Wittmann and M. Zitterbart. *Multicast Protokolle und Anwendungen.* dpunkt, 1999. ISBN 3-920993-40-3.

[170] A. Wolisz. Wireless Internet Architecture: Selected Issues. In *Proceedings of Conference on Personal Wireless Communications (PWC'2000)*, pages 1–16, Gdansk, Poland, September 2000.

[171] J. Wu and G. Q. Maguire Jr. Agent Based Seamless IP Multicast Receiver Handover. In *Proceedings of Conference on Personal Wireless Communications (PWC'2000)*, pages 213–225, Gdansk, Poland, September 2000.

[172] XCast. `http://www.xcast-ig.org/`.

[173] G. Xylomenos and G. C. Polyzos. IP Multicasting for Wireless Mobile Hosts. In *Proceedings of the IEEE Military Communications Conference (MILCOM'96)*, pages 933–937, Washington, DC, USA, November 1996.

[174] G. Xylomenos and G. C. Polyzos. IP Multicast for Mobile Hosts. *IEEE Communication Magazin (Special Issue on Internet Technology)*, 35(1):54–58, 1997.

[175] G. Xylomenos and G. C. Polyzos. IP Multicasting for Point-to-Point Local Distribution. In *Proceedings of the Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom'97)*, pages 1382–1389, Kobe, Japan, April 1997.

[176] G. Xylomenos and G. C. Polyzos. IP Multicast Group Management for Point-to-Point Local Distribution. *Computer Communications, Elsevier Science*, 21(18):1645–1654, 1998.

[177] X. Zhao, C. Castelluccia, and M. Baker. Flexible Network Support for Mobile Hosts. *MONET Special Issue on Management of Mobility in Distributed Systems*, 6(2):137–149, 2001.