UNIVERSIDAD CARLOS III DE MADRID

DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

TESIS DOCTORAL

Mecanismos de Control para Terminales Móviles en Entornos de Tecnologías de Acceso Heterogéneas

Autor: **Antonio de la Oliva Delgado**
Ingeniero de Telecomunicación

Director: **Ignacio Soto Campos**
Doctor Ingeniero de Telecomunicación

Leganés, Mayo de 2008

UNIVERSIDAD CARLOS III DE MADRID

DEPARTMENT OF TELEMATICS ENGINEERING

PhD THESIS

Control Mechanisms for Mobile Terminals in Heterogeneous Access Technology Environments

Author: **Antonio de la Oliva Delgado, MsC**

Supervisor: **Dr. Ignacio Soto Campos**

Leganés, May, 2008

MECANISMOS DE CONTROL PARA TERMINALES MÓVILES EN ENTORNOS DE TECNOLOGÍAS DE ACCESO HETEROGÉNEAS

CONTROL MECHANISMS FOR MOBILE TERMINALS IN HETEROGENEOUS ACCESS TECHNOLOGY ENVIRONMENTS

Autor: Antonio de la Oliva Delgado
Director: Prof. Dr. Ignacio Soto Campos

Tribunal nombrado por el Mgfco. y Excmo. Sr. Rector de la Universidad Carlos III de Madrid, el día ___ de _____ de _____.

Firma del tribunal calificador:

Firma:

Presidente:

Vocal:

Vocal:

Vocal:

Secretario:

Calificación:

Leganés, ___ de _____ de _____.

A mi familia,
a Julia,
a mis amigos y compañeros,
sin los cuales no habría llegado hasta aquí.

En el fondo, los científicos somos gente con suerte:
podemos jugar a lo que queramos durante toda la vida.
– Lee Smolin

La vida es dura.
– Ignacio Soto

Agradecimientos

A lo largo de los años que he invertido en realizar esta tesis he recibido apoyo de muchas personas sin el cual no habría podido terminar este trabajo.

En primer lugar a Julia, gracias por tu infinita paciencia, cariño y apoyo constante. Gracias por apoyarme en las decisiones que he tomado a lo largo de estos años, esta tesis no la habría podido hacer sin ti. Gracias también a mis padres y hermana (y al enano!!) que me han apoyado como siempre lo han hecho.

Un lugar destacado dentro de estos agradecimientos se lo debo a los que considero mis mentores; Albert, Alberto, María y por supuesto Ignacio. Especialmente a ti, Ignacio, muchísimas gracias por dejarme aprender de ti un millón de cualidades, y gracias por tu inagotable paciencia y generosidad. También quiero agradecer especialmente a Carlos, Telemaco y Paulo, el placer de conocerlos y llamarlos amigos. Carlos, cosota, gracias por tu apoyo y buenos consejos que me han acompañado hasta el momento.

A mis amigos de siempre, Nata, Adri, Jacobo, Roberto (Ampa), Toñejo, Vero, Iñigo, Paloma, Pa, y Chus, gracias por aguantar mis interminables rayadas (aunque seguiré!!) y ausencias prolongadas.

A los miembros del Departamento de Telemática de la Carlos III, por lo feliz que me hace trabajar en este ambiente inmejorable. En especial muchas gracias a Pablo, Isaías, Marcelo, Ricardo, Iván, Isaac, Manuel, Carmen, Iria, Jaime, Paco, José Félix, David y Arturo.

Abstract

Internet is evolving to become mobile and ubiquitous. As a consequence, there is a trend towards a diversification of the access technologies, as it can be seen with the recent appearance of wireless technologies such as WiFi or UMTS and the future deployment of WiMAX. Following these new opportunities, multi-technology terminals able to connect to the Internet through different technologies are appearing in the market. In this scenario, users start to demand new solutions able to use these new technologies in a transparent way from the user point of view.

Foreseeing this demand, the IEEE started developing the specification IEEE 802.21, which enables multi-technology terminals to handover from one technology to another in a transparent way for the user. This specification has not yet being finished, and its deployment requires from the research community to analyze how to integrate it in current networks, how to achieve maximum benefit from its possibilities, and how to configure its parameters.

In this thesis we propose control mechanisms for IP terminals to i) support efficient handovers in multi-technology environments applying the 802.21 framework and ii) allow the use of several interfaces and/or multiple providers by the terminals to improve the failure robustness of their communications. These mechanisms are focused in the terminal, although we also provide details on how to integrate IEEE 802.21 into nowadays operator's networks. The contributions of this thesis are threefold. In the first place the integration of 802.21 into terminals has been studied, focusing on the configuration of the parameters required to decide when to perform a handover in the case when the handover is initiated by the terminal. This analysis has also been done taking into account variables such as the terminal speed and the delay of the links. In the second place, we have studied how to introduce the Network Controlled Handover concept, using 802.21, into the network, including the possibility of the handover being initiated by the network. We have analyzed which are the main benefits of this approach and proposed and validated an implementation of this concept in 802.21. In third place we have analyzed a protocol, REAP, under development in the IETF, which allows terminals to detect and recover from failures in the links used in their communications. We have focused in the analytical characterization of the time required to detect a failure, since this parameter is crucial for the application's behavior. The applications should be able to cope with a failure without being disrupted by it. Through the analytical study performed, the REAP protocol can be properly configured to achieve a target recovery time.

All the proposed mechanisms have been validated through simulation, using several tools such as OPNET, OMNET++ and Matlab.

Key words: IEEE 802.21, Heterogeneous networks, Vertical handover, multihoming, Mobility, Failure detection.

Resumen

Las tecnologías de acceso están evolucionando hacia un perfil móvil y ubicuo. Así mismo se está produciendo una diversificación en las tecnologías de acceso disponibles, con la proliferación de tecnologías inalámbricas como WiFi o UMTS y el despliegue próximo de WiMAX. Con la diversificación en el acceso aparecen también los primeros terminales multi-tecnología, capaces de utilizar diferentes redes simultáneamente. En este escenario, los usuarios empiezan a demandar soluciones y servicios capaces de utilizar estas tecnologías de forma transparente al usuario.

Anticipándose a esta demanda, el IEEE comenzó la estandarización de la especificación 802.21 que permitirá a terminales multi-tecnología la posibilidad de realizar traspasos transparentes entre diferentes redes de acceso. Dicha especificación todavía no ha sido completada y su despliegue requiere la investigación de cómo integrarla en las redes actuales, cómo obtener el máximo beneficio de las posibilidades que presenta, así como de la configuración de sus parámetros.

En la presente Tesis Doctoral proponemos una arquitectura que dota a terminales IP de mecanismos de control para i) soportar movilidad eficiente en entornos multi-tecnología en el marco de 802.21 y ii) permitir el uso de múltiples interfaces y/o proveedores con el objetivo de mejorar la robustez ante fallos en las comunicaciones. Dicha arquitectura se centra en el terminal aunque también se aportan detalles de cómo introducir las modificaciones requeridas por IEEE 802.21 en las redes de los operadores. Las contribuciones realizadas son varias. En primer lugar se ha estudiado la integración de IEEE 802.21 en un terminal, centrándonos en la configuración de los parámetros utilizados para determinar el momento del traspaso cuando éste es iniciado por el terminal. En segundo lugar se estudió cómo introducir, usando IEEE 802.21, el concepto de traspaso controlado por la red incluyendo la posibilidad de que la propia red sea la iniciadora del traspaso, analizando sus beneficios y aportando una propuesta de implementación dentro de IEEE 802.21. En tercer lugar analizamos un protocolo, REAP, que se está desarrollando dentro del IETF para permitir, desde los terminales, la detección y recuperación frente a fallos en los enlaces usados en sus comunicaciones. Dentro de este bloque nos centramos en la caracterización analítica del tiempo requerido para detectar un fallo ya que este parámetro es de vital importancia para el funcionamiento de las aplicaciones, que deben poder sobrevivir a un fallo sin verse completamente interrumpidas por él. Con el estudio analítico realizado es posible configurar REAP para alcanzar un tiempo determinado de recuperación ante fallo.

Todos los mecanismos propuestos han sido validados mediante simulación empleando diversas herramientas como OPNET, OMNET++ y Matlab.
Palabras clave: IEEE 802.21, Redes Heterogéneas, Traspaso Vertical, Multi-proveedor, Movilidad, Detección de fallos.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The Internet is evolving to a more ubiquitous network. Users expect to be able to access the Internet anywhere, and use all kind of services, such as voice, TV, video, data, etc. This fact is making operators' networks to evolve towards architectures where all commodity and future services will be transported through a common all-IP core. In order to satisfy end users requirements in terms of mobility and range of services, operators are adopting different technologies in their access networks. In the last few years we have clearly seen a diversification of the access technologies used by operators. Initially, there was only one wireless technology, GSM, allowing users some kind of limited mobile wireless access to Internet. This option has been recently enhanced by the addition of WiFi, GPRS and UMTS. In the near future other promising technologies, such as WiMAX, will enter the market, improving the user capability of connecting to the Internet everywhere. The different service requirements, and characteristics such as density of users, will strengthen the trend towards the adoption of multi-technology access networks by operators.

This thesis envisions a future where a user is able to use a service, such as VoIP, seamlessly performing handovers through different technologies, gaining benefit from the specifics of each technology. In this future the terminals will be smart enough to transparently change the access network the terminal is attached to, running complex algorithms allowing the terminal to know the best timing for the handover in function of its speed, the link characteristics etc. In this future, the network should be able to manage its own resources, controlling the mobility of the users and deciding where and when the terminals must change their point of attachment to the network in order to improve the overall network utilization. Once the terminals are able to handover between different access technologies, and a set of different technologies are available to them, further improvements can be included in the terminal to enhance the user's experience. One of these enhancements is the capability of detecting failures in the links and taking benefit from the avaialability of other links, recover from the failures.

With these requirements in mind, the objectives of this thesis are the following:

i) We first explore the handover initiated by the terminal, analyzing the integration (in a multi-technology terminal) of an upcoming technology, IEEE 802.21, which enables strong interactions between heterogeneous technologies to allow seamless handovers between them. IEEE 802.21 introduces an abstract layer through which

upper layers can obtain information such as events or external information provided by the network, and issue commands in a homogeneous way to different technologies allowing transparent handovers between them. To take full advantage of 802.21, we focus on understanding the interactions between all layers and the proper configuration of link layer thresholds, based in signal level, which trigger control algorithms deciding the timing of the handovers. This allows the flexible adaptation to functional requirements such as maximizing the utilization of the different technologies or minimizing the handover impact in the communications. These decisions are taken while the terminal moves, being the terminal speed one of the main variables affecting the results. For this reason the analysis conducted takes into account the terminal speed and provides results for different speeds, to understand the effect of the change of speed on the algorithm for controlling the handovers.

ii) Secondly, we focus in providing control mechanisms to the network, so the network can be able to manage the mobility of the users as a way of optimizing the resource utilization from the network point of view. This paradigm provides the network with tools to manage the user mobility, deciding to which access point or technology the terminal is attached to. Although the use of this concept places the final decision on the handover target in the network, the handover itself can be initiated by the network or the terminal. In this work, first we have studied the benefits of the network controlled approach, identifying scenarios where the benefit of this approach is maximized. Later we focus on proposing an implementation of this concept in a IEEE 802.21 based network, studying the configuration of the parameters, the signaling overhead and how the delay introduced by the required signaling impacts in the timing and effectiveness of the handovers.

iii) Finally as third objective of this thesis, we focus in the provision of multihoming control capabilities on the terminal. The terminal must be able to use all of its interfaces to provide robustness for its communications. To do this the terminal needs a protocol to timely detect the failure of a path, and to explore and find a new path, through which to resume the communication. We have identified an interesting protocol for this purpose, the REAP protocol, defined in the IETF. This protocol continuously monitors a communication, and it is able to detect a failure in the path followed by its traffic. After a failure has been detected, REAP is able to explore the different paths connecting both end-points of the communication searching for a working path. The interaction between this protocol and upper layers is very important to ensure that the communication is not completely disrupted by the failure. For this reason we have studied the analytical characterization of the protocol. We have developed a mathematical model to obtain the time required by the protocol to detect and recover from a failure in the paths of a communication, according to path and application characteristics. Using this model, REAP can be configured to react in a target time defined by the application requirements. We have also studied the interaction between REAP and TCP.

The above three objectives are the main contributions of this thesis. Although each of the objectives is interesting by itself, we have also defined a terminal and network architecture integrating all the functionality so users can experience a new set of capabilities not present in current terminals.

Following the objectives presented above, this thesis has been organized as follows: Part I presents the protocols and technologies used as building blocks for the architecture presented in this thesis and related research activities. Within this part, chapter 2 focuses in the upcoming standard IEEE 802.21 while chapter 3 presents a state of the art of the related protocols and research work. Part II, chapter 4, presents a terminal architecture which encompass all the contributions of this thesis. Part III, chapter 5, focuses in the Mobile Initiated Handover concept, studying the integration of IEEE 802.21 into a multi-technology terminal and the proper configuration of its parameters. Part IV, chapter 6, studies the Network Controlled Handovers paradigm, identifying scenarios where the concept can provide more benefits and proposing a way of integrating it into IEEE 802.21. Part V, chapter 7, focuses in the analytical characterization of the REAP protocol, providing a model to calculate the time needed by this protocol to detect a path failure and react upon it, also studying the interactions with higher layer protocols such as TCP. Finally part VI concludes this PhD thesis, explaining the conclusions of this work and introducing some relevant future work topics that are open and are worth to be explored in later work.

This PhD Thesis is applying for an ”European Mention” in the PhD Diploma. In order to fully comply with the Spanish (Arts. 11 a 14 del R.D. 56/2005 de 21 de Enero) and University regulations, the entire thesis is written in English and the abstract is also translated into Spanish.

Part I

State of the art

Chapter 2

IEEE 802.21 (Media Independent Handover services) Overview

2.1 Introduction

Several indicators point towards the coexistence of heterogeneous access technologies in the future. Some operators and manufacturers have already taken up the development and introduction of dual-mode and multi-mode handsets to permit connectivity across 3G and WLAN-based networks among other technologies. In such a scenario, future users will expect that their mobile terminal is capable of detecting the different wireless technologies available and selecting the most appropriate one based on the information that the terminal can gather about neighboring cells. In this context, the IEEE is currently working on the specification of a new standard called IEEE 802.21 MIH (Media Independent Handover Services). Although the standard is still not complete, the main lines of the future standard have already been agreed upon. The rest of the chapter is based on the version of the IEEE 802.21 standard draft [1], please note that this standard is a work in progress at the moment so it is possible that some mismatch occurs between the content of this chapter and the definitive version of the IEEE 802.21 standard.
The main purpose of IEEE 802.21 is to enable handovers between heterogeneous technologies (including IEEE 802 and cellular technologies) without service interruption, hence improving user experience of mobile terminals. Many functionalities required to provide session continuity depend on complex interactions that are specific to each particular technology. 802.21 provides in the control plane a framework that allows higher levels to interact with lower layers to provide session continuity without dealing with the specifics of each technology. That is, the upcoming protocol can be seen as the ”glue” between the IP centric world developed in IETF [2] and the reference scenarios for future mobile networks currently being designed in 3GPP [3] and 3GPP2 [4] or other technology specific solutions. Additionally, while IETF does not cover specific layer-2 technologies, 3GPP/3GPP2 only addresses cellular technologies and how to integrate in them upcoming technologies such as WLAN. IEEE 802.21 provides the missing, technology-independent, abstraction layer able to provide a common interface to upper layers, thus hiding technology specific primitives. This abstraction can be exploited by IP stack (or any other upper layer) to better interact with the underlying technologies, ultimately leading to an improved handover performance.

Section 2.2 deepens on the objectives of 802.21. To achieve these goals, IEEE 802.21 defines a media independent entity that provides a generic interface between the different link layer technologies and the upper layers. To handle the particularities of each technology, 802.21 maps this generic interface to a set of media dependent Service Access Points (SAPs) whose aim is to collect information and to control link behavior during handovers. In addition, a set of remote interfaces terminal-network and network-network are defined to convey the information stored at the operator's network to the appropriate locations, e.g. to assist the terminal in handover decisions. All these aspects are covered by the 802.21 reference model and architecture which are explained in section 2.3. All the functionality of 802.21 is provided to the users by a set of services, namely Event, Command and Information services. These services are the core of the specification and define the semantic model of the communication with the lower layers and with the network. A detailed explanation of the services can be found in section 2.4. To conclude the analysis of this technology, section 2.5 presents a use case of inter-technology handover and section 2.6 sketches some open topics currently under development.

2.2 802.21 Objectives

The contribution of the 802.21 standard is centered on the following three main elements:

i. A framework that enables seamless handover between heterogeneous technologies. This framework is based on a protocol stack implemented in all the devices involved in the handover. The defined protocol stack aims at providing the necessary interactions among devices for optimizing handover decisions.

ii. The definition of a new link layer SAP that offers a common interface for link layer functions which is independent of the technology specifics. For each of the technologies considered in 802.21, this SAP is mapped to the corresponding technology-specific primitives. The draft standard includes some of these mappings.

iii. The definition of a set of handover enabling functions that provide the upper layers (like e.g. mobility management protocols such as Mobile IP [5]), with the required functionality for performing enhanced handovers. These functions trigger, via the 802.21 framework, the corresponding local or remote link layer primitives defined above.

Although the main purpose of IEEE 802.21 is to enable the handover between heterogeneous technologies, a set of secondary goals have also been defined. These secondary goals are:

- Service Continuity, defined as the continuation of the service during and after the handover procedure. One of the main goals of 802.21 is to avoid the need for restarting a session after a handover.

- Handover aware applications. The 802.21 framework provides applications with functions for participating in handover decisions. For instance, a voice application may decide to execute a handover during a silence period in order to minimize service disruption.

- QoS (Quality of Service) aware handovers. The 802.21 framework provides the necessary functions in order to take handover decisions based on QoS criteria. For instance, we may decide to handover to a new network that guarantees the desired QoS.
- Network discovery. This is an 802.21 feature that allows providing users with information on the candidate neighbors for a handover.
- Network selection assistance. Network selection is the process of taking a handover decision based on several factors (such as QoS, throughput, policies or billing). In line with the above, the 802.21 framework only provides the necessary functions to assist network selection, but does not take handover decisions which are left to the higher layers.
- Power Management can also benefit from the information provided by 802.21. For instance, power consumption can be minimized if the user is informed of network coverage maps, optimal link parameters, or 'sleep' or 'idle' modes.

2.3 IEEE 802.21 Architecture

In this section we present the general architecture of IEEE 802.21. We describe the different layers in the 802.21 protocol stack and their interaction, both at the node and network level. Figure 2.1 shows the logical diagram of the general architecture of the different nodes in an 802.21 network. It shows a Mobile Node with an 802 interface and a 3GPP one, and that is currently connected to the network via the 802 interface. The figure shows the internal architecture of the Mobile Node, the 802 network, the 3GPP network and the Core Network. As it can be observed from the figure, all 802.21 compliant nodes have a common structure surrounding a central entity called MIHF (the Media Independent Handover Function). The MIHF acts as intermediate layer between the upper and lower layers whose main function is to coordinate the exchange of information and commands between the different devices involved in taking handover decisions and executing the handovers. From the MIHF perspective, each node has a set of MIHF users, which will typically be mobility management protocols, that use the MIHF functionality to control and gain handover related information. The communications between the MIHF and the other functional entities such as the MIHF users and the lower layers are based on a number of defined service primitives that are grouped in Service Access Points (SAPs). Currently, the following SAPs are included in the 802.21 standard draft (see Figure 2.1):

- MIH_SAP: This interface allows communication between the MIHF layer and the higher layer MIHF users.
- MIH_LINK_SAP: This is the interface between the MIHF layer and the lower layers of the protocol stack.
- MIH_NET_SAP: This interface supports the exchange of information between remote MIHF entities.

It is worth to note that all communications between the MIHF and lower layers are done through the MIH_LINK_SAP. This SAP has been defined as an abstract media-dependent

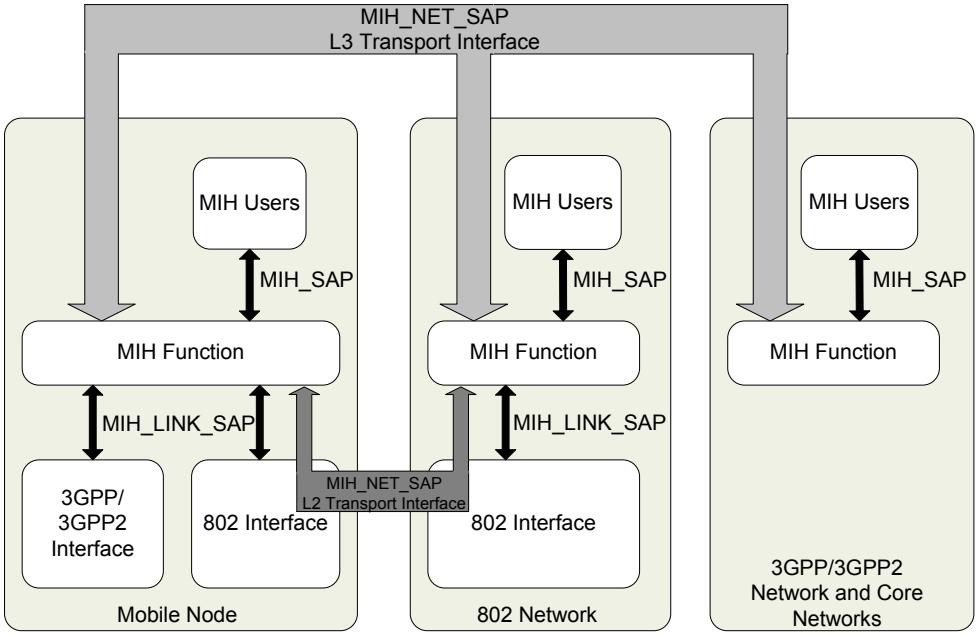


Figure 2.1: 802.21 General Architecture.

interface common to all technologies, so that the MIHF layer can be designed independently of the technology specifics. However, these primitives are then mapped to technology specific primitives offered by the various technologies considered in 802.21. A table with the mapping of the primitives of the MIH_LINK_SAP interface to the link primitives of several technologies is included in the 802.21 draft.
Figure 2.2 presents the 802.21 reference model, which includes the following network entities:

- MIH Point of Service (MIH PoS): This is a network entity that exchanges MIH messages with the Mobile Node. Note that a Mobile Node may have different PoS as it may exchange messages with more than one network entity. This is the case, for instance, in the example of Figure 2.2.
- MIH non-PoS: This is a network entity that does not exchange MIH messages with the Mobile Node. Note that a given network node may be a PoS for a Mobile Node with which it exchanges MIH messages and a non-PoS for a network node for which it does not.
- MIH Point of Attachment (PoA): This is the endpoint of a L2 link that includes the Mobile Node as the other endpoint.

In order to make the communication between these network entities possible, the reference model specifies several communication reference points:

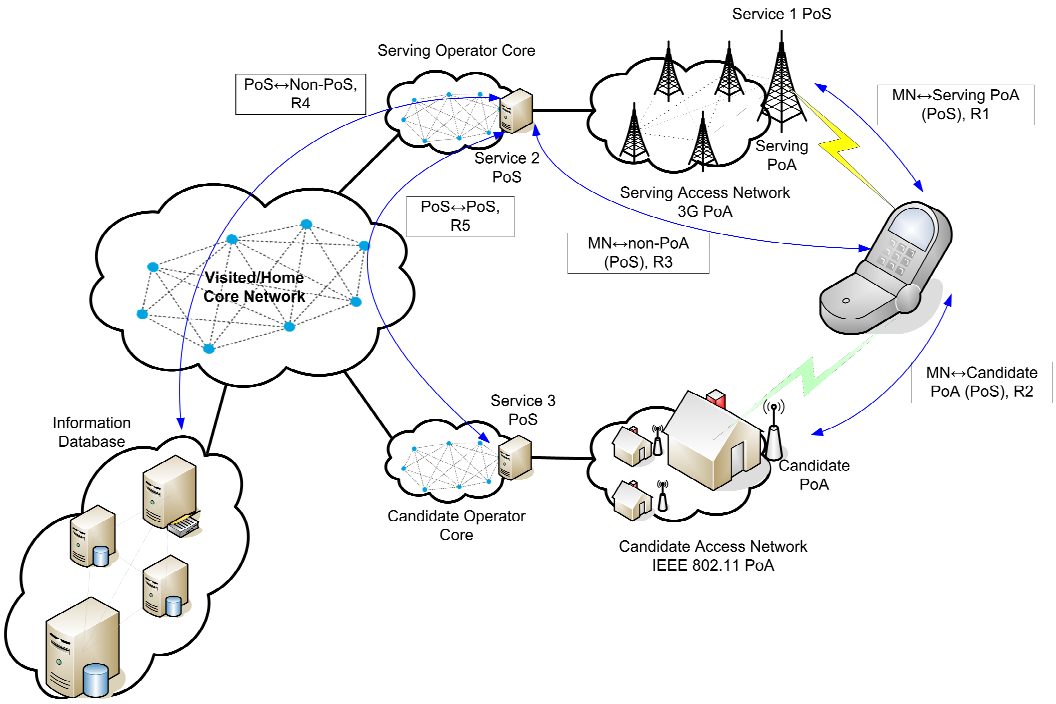


Figure 2.2: Reference Model.

- Communication Reference Point R1 (“MN↔Serving PoA (PoS)”): This communication reference point is used by the Mobile Node to communicate with its PoA. Among other purposes, it may be used by the Mobile Node to gather information about the current status of its connection.
- Communication Reference Point R2 (“MN↔Candidate PoA (PoS)”): This communication reference point is used by the Mobile Node to communicate with a candidate PoA. It may be used to gather information about candidate PoAs before taking a handover decision.
- Communication Reference Point R3 (“MN↔non-PoA (PoS)“): This communication reference point is used by the Mobile Node to communicate with a MIH PoS located on a non-PoA Network Entity. It may be used for example, by a network node to inform the Mobile Node about the different IP configuration methods in the network.
- Communication Reference Point R4 (“PoS↔non-PoS”): This communication reference point is used for communications between a MIH PoS and a MIH non-PoS. This reference point is typically used when a MIH server that is serving a Mobile Node (the PoS) needs to ask for information to another MIH server (the non-PoS).
- Communication Reference Point R5 (“PoS↔PoS”): This communication reference point is used between two different MIH PoS located at different network entities.

For the exchange of information between remote MIHF entities defined by the MIH_NET_SAP interface, some transport protocol is needed. For this transport, 802.21 allows both layer 2 (L2) and layer 3 (L3) communication, as illustrated in Figure 2.1. Note that, when the two MIHF entities are located in the same L2 cloud, both L2 and L3 communications are possible, while otherwise the only possibility is to have L3. Following this, in Figure 2.1 the communication between the mobile terminal and the 802 network is based on L2 transport while the communication outside is based on L3 transport. One of the common uses for L3 transport is to gather information about candidate networks to which the mobile is not currently connected. The communication reference points R1, R2 and R3 can be used for L2 or L3 communication, while communication reference points R4 and R5 may only be used for L3 communication.

2.4 MIH Services

The 802.21 architecture and reference model explained in section 2.3, present a framework which supports a complex exchange of information aiming at enabling seamless handover between heterogeneous technologies. 802.21 defines three different types of communications with different associated semantics, the so called MIH services. The three services are, i)Event services (ES), ii) Command Services (CS) and iii) Information Services (IS). These services allow the MIHF users to access handover related information as well to deliver commands to the link layers or to the network. The MIH services can be delivered in an asynchronous or synchronous way. Events generated in link layers and transmitted to the MIHF or MIHF users are delivered by an asynchronous method, while commands and information, generated by a query/response mechanism are delivered in a synchronous way.

2.4.1 Media Independent Event Service

The IEEE 802.21 supports handover initiated by the network or the mobile terminals, hence, events related with handovers can be originated at the MAC layer or MIHF layer located in the node or at the point of attachment to the network. As several entities could be interested in the generated events, the standard specifies a subscription delivery mechanism. All entities interested in an event type should register to it, when the event is generated it will be delivered to the subscription list. MIH remote events may be delivered using the R1 (“MN↔Serving PoA (PoS)”), R2 (“MN↔Candidate PoA (PoS)”) and R3 (“MN↔non-PoA (PoS)“) reference points of the model explained in section 2.3.
It is important to note that an entity is not forced to react on the reception of an event, being event’s nature advisory.
Events can be divided in two categories, Link Events and MIH Events. Link Events are generated within the link layer and received by the MIHF. Events that are propagated by the MIHF to the MIHF users are called MIH Events. Note that Link Events propagated to upper layers become MIH Events. Entities being able to generate and propagate Link Events are the defined IEEE 802.x, 3GPP and 3GPP2 MIH_LINK_SAP interfaces.
The Media Independent Event Service (MIES) can support several event types:

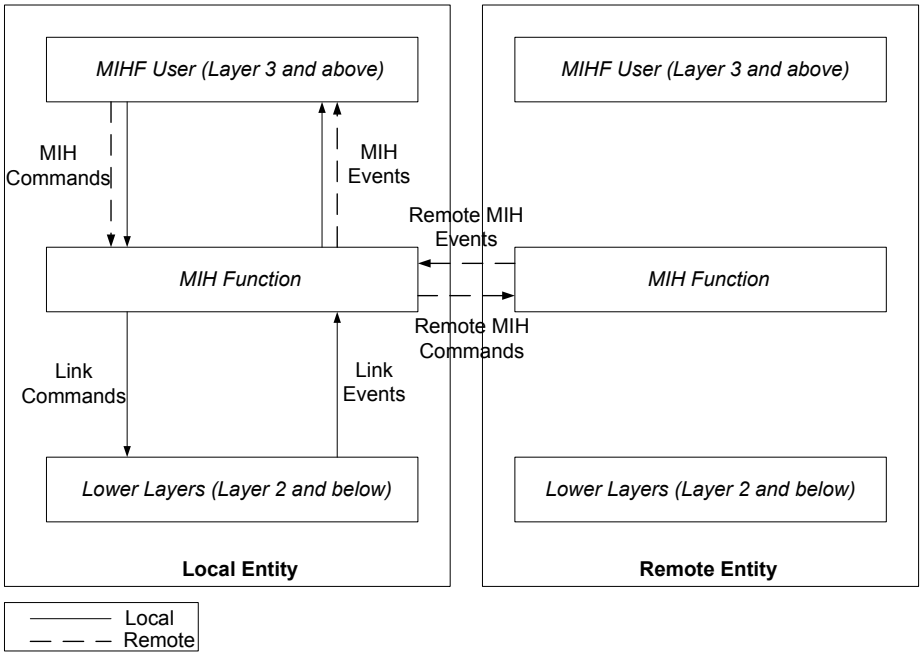


Figure 2.3: Event, command and information services flow mode.

- MAC and PHY State Change events: These events inform about a definite change in the MAC or PHY state. Examples of this type of events are the Link Up or Link Down events.

- Link Parameters events: These events are generated due to a change in the link layer parameters. They can be generated in a synchronous way (a parameters report on a regular basis) or by an asynchronous method like reporting when a specific parameter reaches a threshold.

- Predictive events: Predictive events are used to inform the system of the likelihood of change in the link properties based on the previous history and present conditions. For example, a decay in the wireless signal level could indicate a future failure in the link. These events may carry information about time bounds or confidence intervals to help in the decision making.

- Link Synchronous events: These events report deterministic information about link layer activities that are relevant to higher layers. The information delivered does not need to be a change in the link parameters, it can be indications about link layer activities such as the native link layer handover methods which are performed autonomously by the link layer, independently from the global mobility protocol.

- Link Transmission events: These events inform of the transmission status of higher layers PDUs by the link layer. By these events, the link layer may inform the higher layer of the losses in the ongoing handover. This information can be used to dimension

the buffers needed for seamless handover or to adopt different retransmission policies at higher layers.

The communication flow followed by events is shown in Figure 2.3. As an example of use, event services are helpful to detect when a handover is possible. There are several events such as Link Up, Link Down or Link Parameters Change that could be used to detect when a link has become available or when the radio conditions of this link are appropriate to perform a handover to this new link.

2.4.2 Media Independent Command Service

The Media Independent Command Service (MICS) refers to the commands sent from the higher layers to the lower layers in order to determine the status of links or control and configure the terminal to gain optimal performance or facilitate optimal handover policies. The mobility management protocols should combine dynamic information regarding link status and parameters, provided by the MICS with static information regarding network status, network operators or higher layer service information provided by the Media Independent Information Service, to help in the decision making. The receipt of a certain command request may cause event generation, and in this way the consequences of a command could be followed by the network and related entities. Commands can be delivered locally or remotely. Through remote commands the network may force a terminal to handover, allowing the use of Network Initiated Handovers and Network Assisted Handovers. A set of commands are defined in the specification to allow the user to control lower layers configuration and behavior, and to this end some PHY layer commands have being specified too. The communication flow mechanism is shown in figure 2.3. MIH remote commands may be delivered by the R1 ("MN↔Serving PoA (PoS)"), R2 ("MN↔Candidate PoA (PoS)"), R3 ("MN↔non-PoA (PoS)") and R5 ("PoS↔PoS") reference points.
Commands are classified into two main categories:

- MIH Commands: These commands are sent by the higher layers to the MIHF, in the case the command is addressed to a remote MIHF, it will be sent to the local MIHF which will deliver the command to the appropriate destination through the MIHF transport protocol. To enable network initiated handovers as well as mobile initiated handovers, the command service provides a set of commands to help with network selection. Examples of such commands are MIH Handover Initiated or MIH Handover Prepare. It is worth to notice that all these commands do not affect the routing of user packets. All commands are designed to help in the handover procedure but the routing of the user packets is left to the mobility management protocols located at higher layers, like Mobile IP or SIP [6].

- Link Commands: These commands are originated in the MIHF, on behalf of the MIH user, in order to configure and control the lower layers. Link commands are local only and should be implemented by technology dependant link primitives to interact with the specific access technology. New link commands shall be defined as amendments to the current technology standards.

2.4.3 Media Independent Information Service

Media Independent Information Service (MIIS) provides a framework through which an MIHF located in a user terminal or in the network is able to acquire network information within a geographical area to facilitate handovers. The objective is to gain knowledge about all heterogeneous networks in the area of interest of the terminal to facilitate handovers when roaming across these networks. MIIS is based in Information Elements (IEs) and these elements provide information essential to the network selection algorithm to make a successful handover across heterogeneous networks and technologies. The information provided by the IEs can be related to lower layers such as neighbor maps, coverage zones and other link parameters. Information related with higher layer services such as lack of Internet connectivity in certain zones or availability of certain services may also be provided. MIIS is designed to provide information mainly about 802, 3GPP and 3GPP2 networks, although this list may be extended in the future. All the information related not only to the technology the mobile node is currently attached to, but the surrounding available technologies can be accessed from any single technology. As an example, a MN connected to an 802 network such as WiFi, will be able to gather information about the 3G cellular network within its geographical area, without the need to power up its 3G interface to obtain this information. This characteristic allows an optimal power utilization. The main goal of MIIs is to provide the MN with essential information that may affect the selection of the appropriate networks during a handover. The information provided by this service is intended to be mainly static, primary being used by policy engines which do not require dynamic and updated information, although network changes may be accounted for. The dynamic information about the active networks should be obtained by the use of the MIH Event and Command services explained in sections 2.4.1 and 2.4.2. The Information Elements (IE) provided by the MIIS can be divided in the following groups:

- General Information: These IEs give a general overview about the networks covering a specific area such as network type, operator identifier or service provider identifier.
- Access Network Specific Information: These IEs provide specific information for each technology and operator. The information is related to security characteristics, QoS information, revisions of the current technology standard in use, cost, roaming partners etc..
- Point of Attachment (PoA) Specific Information: These IEs provide information for each PoA (for each technology and operator). The information comprises aspects like MAC address of the PoA, geographical location, data rate, channel range etc..
- Higher Layers services/information per PoA: The information provided is related with the available services on this PoA and network. The information provided may be the number of subnets this PoS support, the IP configuration methods available, or even a list of all supported services of the PoA.
- Other Information can be added, like vendor specific information or services.

It is important to note that the MN should be able to discover whether the network supports IEEE 802.21 by the use of a discovery mechanism or information obtained by MIIS

through another interface. It is also important that the MN is able to obtain MIIS information even before the authentication in the PoA is performed in order to be able to check the security protocols, support of QoS, or other parameters before performing a handover. The communication between the different entities of the IEEE 802.21 network in order to gather information related to the MIIS may be performed through all the communication reference points defined in section 2.3.

2.5 Use case: Inter-technology Handover procedure

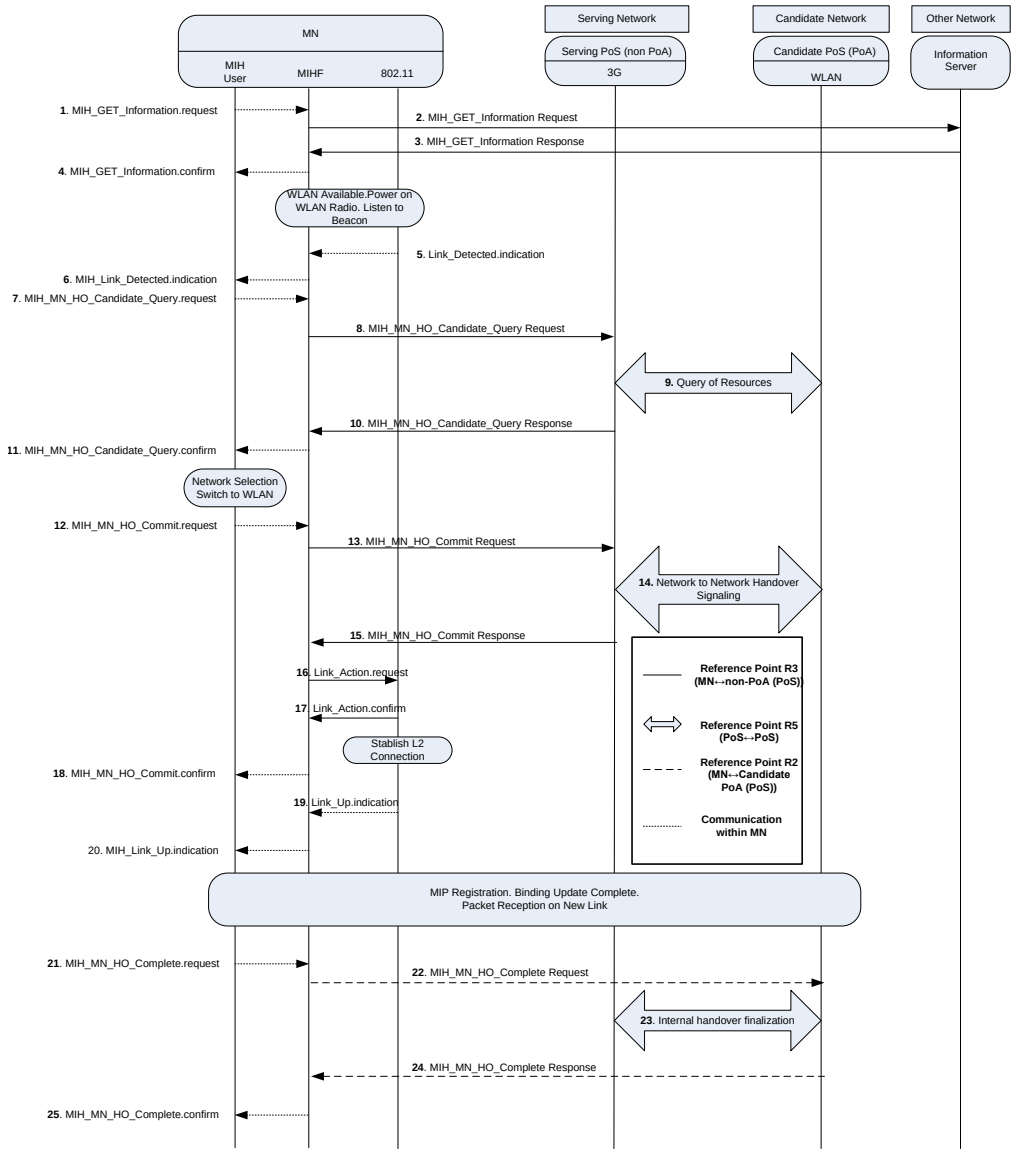


Figure 2.4: Inter-technology Handover Example.

Figure 2.4 shows the message exchange involved in a mobile initiated handover from

3G to WLAN. In the following a detailed explanation of the messages and procedures is presented:

- The handover procedure starts by the MIH User of the MN querying the MIHF located on the MN itself about the surrounding networks (message 1). This query is forwarded by the MIHF to the information server located in the operator network (or a third party network). The query is started by message 1 and answered by message 4. Through these four messages the MN gets the required information in order to gain an understanding of the networks to which perform a handover while roaming through this specific geographical area. As the answer contains information regarding a possible WLAN network, the MN switches on its WLAN interface and starts listening for beacons.

- Once a beacon is received, the IEEE 802.11 link layer will generate a Link_Detected.indication event (message 5). The link layer, through an IEEE 802.11 defined primitive, indicates the detection of a new link. This primitive is mapped into the event through the use of the MIH_LINK_SAP. This indication is forwarded by the MIHF to the MIH User on message 6.

- When the MIH User receives the MIH_Link_detected.indication, it triggers the mobile-initiated handover by sending to its PoS (located on the 3G network) the information regarding potential candidate networks discovered up to the moment. This information is sent on message 7 to the MIHF which forwards this query to the serving PoS (message 8).

- After receiving message 8, the serving PoS starts querying the available candidate networks (taking into account the information provided by the MN) asking for the list of resources available and including the QoS requirements of the user (exchange 9). This is performed by a successive exchange of Query_Resources messages with one or several candidate PoSs. The result of the queries is sent to the MN through message 10 and 11. At this point, the MN has enough information about the surrounding networks to take a decision on the network to which to hand over.

- Once the MIH User has decided the target network to hand over, it delivers a Handover Commit command to the MIHF (message 12). This message is used to inform the network of the decision taken by the Mobile Node. The message is then propagated through the network via message 13. After reception, message 13 triggers a sequence of messages within the network side which informs the different entities involve of the handover request (message sequence 14). Once the network has been informed and no constrains have been found, message 15 is issued, informing the Mobile Node of the successful completion of the handover information through the network.

- At this point the Mobile Node is able to start the L2 connection. It issues a message to the lower layers indicating that a handover must start, powering up the interface and other required operations (message 16), this message is confirmed through message 17.

- Once the connection process has been started, the MIHF informs the MIH User of the completeness of the process (message 18), although this message only confirms the starting of the handover process.

- Once the connection is established, the WLAN MAC layer issues an event reporting the end of the L2 handover to the MIHF (message 19) which will be forwarded to the MIH User (message 20).

- Once message 20 is received a higher layer handover procedure can start. In this case Mobile IP has been selected, although any other mobility management protocol would be equally suited.

- When the handover is completed at the higher layers, the MIH User sends a MIH_MN_HO_Complete.request message to the MIHF which will inform the target PoS (message 22) which becomes the new serving PoS. At this point the target PoS informs all the implied network entities of the handover finalization (exchange 23). Specifically, the Target PoS has to inform the serving PoS of the handover completion so it can release any resources.

- Finally message 24 closes the handover procedure, indicating to the MN that the procedure has finished, and message 25 informs the MIH User.

2.6 Summary, Contributions and Open Issues

On this section, we have provided an overview of the current status of the upcoming IEEE 802.21 specification. The IEEE 802.21 aim is to enable inter-technology handovers maximizing session continuity as a way of improving users' satisfaction while using mobile terminals in heterogeneous environments. Mobile terminals are used worldwide nowadays, and even more, terminals with several interfaces and access technologies are starting to be introduced in the market. Envisioning such scenario, the IEEE 802.21 specification will play an important role on near future communications, providing technological solutions for layer 2 inter-technology handovers and interfaces with layer 3 mobility solutions.
Open issues include the integration of 802.21 with the IP transport layer for layer three transport. In the IETF MIPSHOP WG [7] efforts are currently undergoing to specify a protocol for mobility services transport. Documents [8], [9], [10] or [11] give general statements on what issues the solution space document should address.
Another open issue not addressed in 802.21 is the use of other transport technologies to carry 802.21 transactions. A typical scenario could include a layer two transport (802 networks) on the wireless link up to the PoA, and a layer three transport between the PoA and the PoS. Such scenario is referred in the draft as proxy scenario. Initially proposed for information services only, in [12] the authors propose to use the same mechanisms as well for event and command services. Utilizing such an approach brings a certain number of advantages. Since the proxy method allows two MIH peers to complete a handshake while one of the peers contacts a third MIH peer to make information available at the requesting peer, the mobile node implementing the MIHF does not need to discover a specific IS/ES/CS server when it contacts its default up-link MIH peers (discovered via 802.21 specific mechanisms).

Such mechanism while simplifying layer three discovery of IS/ES/CS services at the mobile node side, also provides a certain level of privacy from the network perspective (i.e. the operator does not disclose topology related information). An alternative application of the proxy scenario is the centralized approach for network initiated handovers discussed in [13]. In fact, while the current draft does not prevent the execution of NIHO, a more optimized approach could be possible with slight modifications to the current specifications. Thus, the document [13] presents the necessary modifications, namely better network to network message exchange, enabling a centralized mechanism for network controlled and initiated handovers.

The author of this thesis has participated in some contributions to the IEEE 802.21 standard. In [14] the authors propose to extend the Event Service of 802.21 to support also events generated by MIH Users. At the moment of this contribution the specification explicitly defined the Event Service as a communication exclusively originated from Link Layers to MIHF or from MIHF to MIH users. This contribution started a discussion on the working group which led to the current model of communication where the events can also be triggered by special commands sent by the MIH-users. In [15] the authors propose the inclusion of the mesh technology inside the scope of the 802.21 standard.

The IEEE 802.21 standard is currently being finalized, hence there is a lack of experience with this technology. Specifically, at the beginning of this thesis, there was no experience on implementing the MIHF. The use of link layer triggers within the 802.21 framework to decide when to perform handovers had also not being studied yet. The IEEE 802.21 also does not provide decision algorithms, while traditional ones are based in a limited set of information and typically thought for monotechnology environments, but 802.21 offers a complete new set of parameters and information that can be used in multitechnology environments. Proper analysis of the configuration of the triggers, the proper timing of the handovers (related with the value of the thresholds used to start them) or the variation of this configuration when the user changes from an almost steady state to a fast moving state is required in order for this technology to reach its objectives of providing seamless handovers.

Finally the integration of the IEEE 802.21 technology into the operator's core where a strict control of the terminal behavior is needed had still not been considered, being needed the integration of the Network Controlled mobility paradigm within this technology, accounting for the required new signaling.

Chapter 3

IP Mobility and Multihoming Support Overview

The mechanisms presented in this thesis use several protocols as building blocks, combining them into an integrated solution for mobility control in heterogeneous environments. In this chapter we present an outline of the protocols used along this thesis to enable mobility and multihoming in the terminals of the future Internet, along with some architectures introduced in the literature trying to solve, at least partially, the problems of multihoming and mobility across heterogeneous networks.

3.1 Enabling Mobility in the Internet

In the past years the access technologies used to connect to the Internet have been dramatically changed. From an access paradigm on which the majority of users used modems to connect to the network, nowadays the broadband has reached the homes and with it a major deployment of wireless technologies. ADSL has become the basis of connectivity of millions of homes and offices, and with it a great number of WiFi Access Points has been deployed. Every laptop and a lot of mobile terminals are able to connect to the Internet via wireless technologies. This fact added to the possibilities of the huge quantity of mobile phones starting to use Internet based services [16] [17] [18], highlight the trend to integrate voice services on Internet, encouraging the need of a Mobility Management protocol for the IP layer.

On the current Internet the nodes attaching to the network on any location obtain an IP address via DHCP [19] or other mechanisms, but this IP address does not allow the node to be reachable from a well known address, stored for example in the DNS [20] [21], and even more, established connections are closed when the node changes its point of attachment since upper layers (UL) use the IP address as part of the connection identifier (ULID) and if it changes, the connection is not longer valid. These problems arise due to the design of the protocol stack itself, on which the IP address plays two simultaneous roles, identifier and locator.

Taking into account these problems and foreseeing the future uses of the Internet, the requirements [22] of a mobility solution are:

- Session Continuity: Sessions opened between two hosts must not be dropped when a node changes its point of attachment to the Internet. This requirement introduces the problem of interfacing with higher layers in order to provide them with a static identifier which does not change during the session lifetime independently of the point of attachment to the network.
- Reachability: A node must be always reachable through a well known address (such as the ones stored in the DNS) wherever it is connected to the Internet. This requirement introduces the need of a Rendezvous element into the architecture.
- Application Independence: In order for the mobile solution to be globally adopted, it cannot require changes to the applications. The use of mobility functionality must be transparent to higher layers.
- Lower Layers Independence: The mobility solution to be widely deployed must not add any restriction to the lower layers, or some end user equipments may not be able to adopt it.
- End to End Signaling: The mobility solution must hold into the current Internet model. On this model, the Internet is formed by end hosts and routers. Routers are in charge of forwarding the packets to the required destination and no further functionality must be added to them.

Once the requirements for the mobility solution are clear, another question arises. At which layer of the protocol stack must the mobility be handled? [23]. This question is a source of strong discussions between the supporters of each solution. There are several approaches to address the mobility problem, at the Link Layer (MAC solutions), at the IP layer, or at transport or application layer.
Link layer solutions for mobility exist nowadays, every Wireless LAN technology allows the movement of nodes on its boundaries. The problem with this type of mobility management is when mobility between different technologies (such as a handover between a WiFi ad 3G network) is desired.
To support mobility management at transport layers new transport protocols must be designed or current ones must be modified in a way such as them do not rely in the used IP addresses as identifiers (such as SCTP [24] [25]). This allows the modification of the IP address used at the IP layer without affecting the identifier of the connection at transport layer, thereby enabling the change of the IP address (mobility) without impacting established communications. The problem with this solution is that it implies changing the transport protocol, which also affects the interface with applications. This seriously affects the feasibility of the deployment of the solution.
Managing the mobility at Application layer is also possible but it would require the rewriting of every application that need mobility support. If a wide deploy of the mobility solution is desired, this does not seem the best approach.
Finally another possibility is to handle the mobility at IP layer. If we revisit the problem we will understand why this has been one of the approaches finally adopted by the IETF. The main problem is that after a movement, a node cannot receive any packet. The reason is that the destination address of these packets, after a movement, does not correspond topologically to the new node location. This problem is not particular to any application, transport

protocol or link layer, being inherent to the IP protocol. It seems reasonable then to handle the mobility where the problem arises, in the IP layer.
With these ideas in mind, the IETF started on the mids 1990s the designing of a mobility management protocol for the upcoming version 6 of the IP protocol (IPv6 [26]). This new protocol or extension to the IPv6, called Mobility Support in IPv6, was finally standardized as RFC 3775 [5] in June 2004.

3.1.1 Mobility Support in IPv6

The Mobility Support in IPv6, known as Mobile IPv6, enables nodes to maintain ongoing communications and remain reachable while changing its point of attachment to the IPv6 network. Figure 3.1 presents the basic functionality of this protocol.

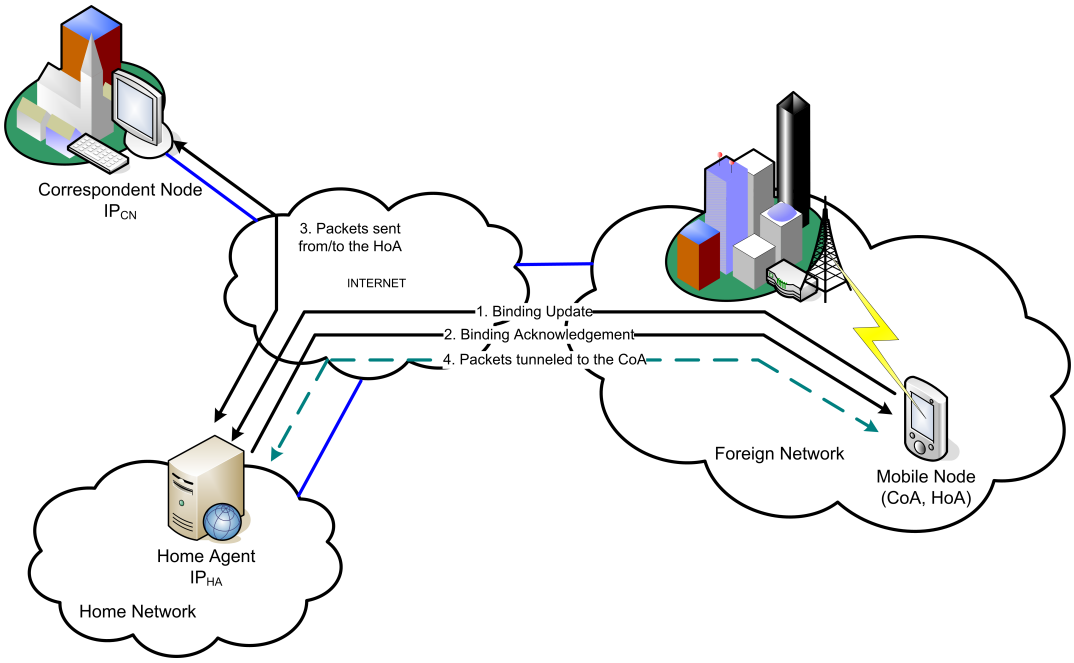


Figure 3.1: Mobile IPv6 Tunnel Mode

A Mobile Node (MN) is always expected to be attached to its Home Network, on which it has an address named Home Address (HoA). This address is the one used to send packets to the MN and it is a well known address suitable to be stored in a DNS. Packets sent to the MN are routed to the HoA by normal routing means. Once a node moves to a Visited Foreign Network, it attaches to the network and obtains a new topologically correct address belonging to the Visited Foreign Network. This address is called the Care-of Address (CoA) and it can be used to communicate with the MN while it is in the Visited Foreign Network. Packets addressed to the CoA will reach the Mobile Node as long as it stays on the Foreign Network. Note that the MN can obtain one or several CoAs at the Visited Foreign Network, i.e. depending on the number of prefixes advertised by the network. The CoAs can be obtained by standard stateless or stateful mechanisms.
In order to be able to receive packets addressed to the HoA, the MN must associate the

CoA to the HoA. This association is known as a binding. In order to create the binding, the MN registers its primary CoA with a router located in the Home Network. The MN sends a Binding Update message (see message 1 in figure 3.1) to a router at its Home Network, requesting it to act as a Home Agent (HA) for packets sent to the MN's HoA. In case of agreement, the HA sends a Binding Acknowledgment (see message 2 in figure 3.1) to the MN, acknowledging the establishment of the binding.
The communication with any peer node, called Correspondent Node (CN), can be hold in two modes, the first one corresponds to the basic operation that does not require any mobility support on the CN, it is called Bidirectional Tunnel Mode. The second one requires Mobile IP support on the CN and performs an optimization of the path followed by the packets, to increase the performance of the routing. This second mode is called Route Optimization Mode. A specific security procedure, know as Return Routability procedure is used to provide the needed security on this solution. We will see the operation of this optimized mode later, now we focus on the tunnel mode.
Once the binding is established (in Tunnel Mode), packets addressed to the HoA will reach the Home Network (see message 3 in figure 3.1). The HA uses Proxy Neighbor Discovery [27] to capture the packets addressed to the HoA and forwards them to the MN by an IP on IP tunnel. This tunnel encapsulates the packets (IP source address: IP_{CN}, IP destination address: HoA) into another IP packet with IP source address, the IP_{HA}, and IP destination address, the CoA. Once a packet arrives to the MN, it is extracted from the tunnel and handled to the upper layers. All traffic originated by an application using the HoA as source address is reverse tunneled to the HA which forwards the packets back to the CN.
As expected, this mode of operation has several drawbacks, such as the increased overhead and delay. For these reasons, the IETF designed a Route Optimization solution which overcomes the drawbacks of the basic solution. The Route Optimization mode relies on the support of Mobile IP in the CN. Basically the MN registers its CoA also in the CN so packets exchanged between them can be sent directly without travelling through the HA. The overhead of this solution is much smaller than the basic solution since just a routing header type 2 (carrying the HoA of the MN [28]) is added to the packet and traffic goes directly from CN to MN and from MN to CN. When the MN receives a packet from the CN, it explores the packet and finds the routing header type 2. Then it extracts the HoA from the routing header and modifies the destination address of the packet accordingly. Then it forwards the packet to higher layers.
The use of the Route Optimization Mode has some security implications, being the main problem the possibility of a malicious node stealing traffic destined to a MN or the ability of performing Denial of Service (DoS) attacks by redirecting the flows of a CN to a MN. Basically if there is no security mechanism to assure the relation of a HoA and CoA, a malicious user may redirect all packets sent by a CN to other address, performing a DoS attack. To solve this issue, the IETF designed a security mechanism, known as Return Routability procedure through which a CN can establish the relation between the CoA and the HoA by checking that packets sent to the CoA and the HoA reach the same node. Figure 3.2 presents an example of utilization of the Return Routability procedure, and the messages involved on it.

The Return Routability procedure consist on the exchange of 5 messages, the Home Test Init (HoTI), the Care-of Test Init (CoTI), the Home Test (HoT), the Care-of Test (CoT) and

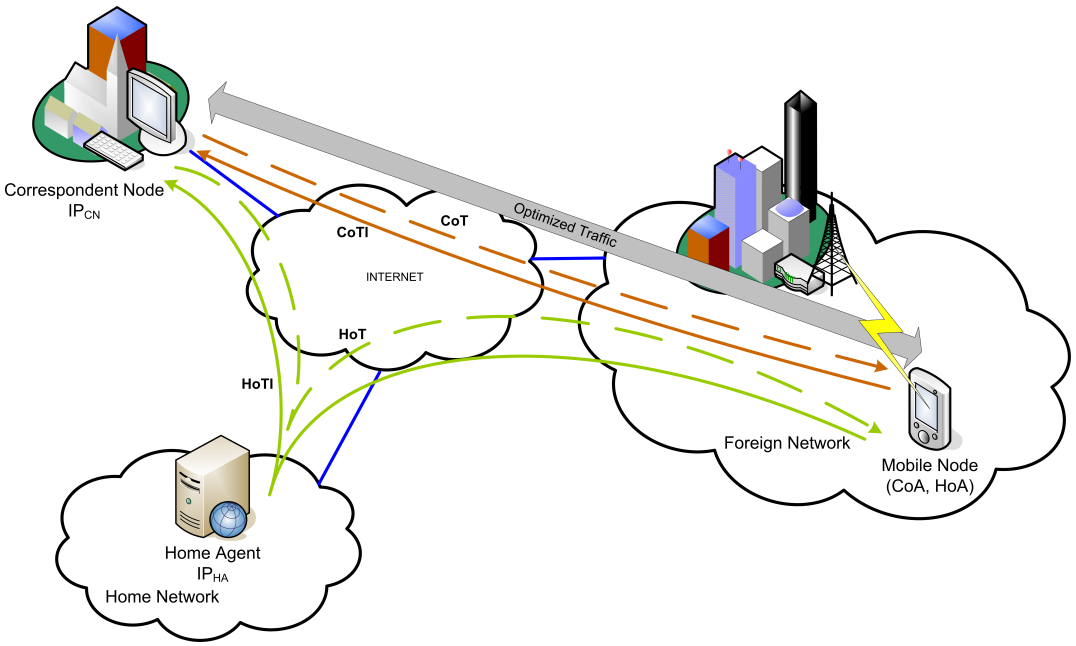


Figure 3.2: Mobile IPv6 Routing Optimization Mode

the Binding Update (BU). The mechanism is started once the communication between a CN and a MN is established and the packets are flowing between them via the tunnel at the HA. At some point, the MN decides to start a Return Routability procedure and sends the HoTI message through the tunnel to the CN. The HoTI message has as source address the HoA, as destination address the IP$_{CN}$ and a parameter called the home init cookie. The home init cookie must be returned later by the CN to assure the MN is talking with the desired node. In parallel with the HoTI, the CoTI is also sent by the MN. This message is sent directly to the CN without transversing the tunnel to the HA. This packet has as source address the CoA, as destination address the IP$_{CN}$ and a parameter called care-of init cookie. Once the HoTI has reached the CN, it sends a HoT message to the MN. This message, via normal routing procedure, will reach the HA which forwards it to the MN. This message has as source address the IP$_{CN}$, as destination address the HoA and it carries three parameters. These parameters are the home init cookie, the home keygen token and the home nonce index. The home init cookie corresponds to the cookie sent by the MN. The second parameter, the home keygen token is generated as follows:

$$home\ keygen\ token = First_{64bits}(HMAC\_SHA1(Kcn, (homeaddress \| nonce \| 0)))$$

The home keygen token is formed by the first 64 bits of a MAC function, with key Kcn, of a concatenation of the home address, a nonce and 0. The home nonce index corresponds to the index of the nonce used on the above calculation. The home keygen token allows the CN to verify that messages sent to the CoA reach the HoA and vice versa.

Coming back to the Return Routability procedure, once the CN receives the CoTI, it sends a CoT message. This message is sent directly to the CoA so it carries the CoA as destination address, IP$_{CN}$ as source address and three parameters as the HoT. These parameters are the care-of init cookie, the care-of keygen token and the care-of nonce index. As in the HoT

message, the care-of init cookie corresponds to the cookie sent by the MN on the CoTI message. The care-of nonce index corresponds to the index of the nonce used on the calculation of the care-of keygen token, and the care-of keygen token is calculated in a similar way as the home keygen token (but using 1 instead of 0 to differentiate between both).
Once the MN receives both messages, the HoT and CoT, the Return Routability procedure is complete. As result of the procedure, the MN has all the data needed to obtain a key, which included in a Binding Update message sent to the CN, allows the binding to be created. This key is obtained by performing the hash of the concatenation of the home keygen token and the care-of keygen token. Note that the CN does not store this key or creates any state prior to the reception of a Binding Update message. All the required state and the generation of the key to validate the binding is created when the Binding Update is received.
Once the binding has been established, both nodes can start sending the packets directly to each other, without the previously required pass through the HA. To reduce the risk of a malicious MN performing the Return Routability process with a spoofed address and then leaving the network and effectively performing a DoS attack, the validity of an optimized binding is limited to seven minutes. When this time expires a new Return Routability procedure must be performed or the protocol operational mode will revert to Tunnel Mode.
Regarding the use of the Mobile IP protocol on real terminals, there is one consideration that must be noted. As explained on the previous paragraphs, Mobile IP allows a maximum of one CoA bound to a HoA. Modern terminals, such as smart phones, have more than an interface and nothing prevents the terminal to obtain more than one CoA. In order to take benefit of the multiplicity of CoAs and being able to use flow binding or multihoming with Mobile IP an extension to this protocol is being developed by the IETF. This extension is called Multiple Care-of Addresses registration [29].
So far Mobile IPv6 has been considered as the main IP mobility management, this fact does not mean Mobile IPv6 is free of drawbacks. Mobile IPv6 was designed to provide basic macroscopic mobility but it is not well suited for micro-mobility, being this one of its major drawbacks. The time required to update the binding with the HA once a L2 handover is performed corresponds to a Round Trip Time (RTT). If the HA is far away from the Visited Foreign Network or the technology being used have an inherent long RTT (like GPRS or UMTS connections), this time can be very long, producing a high packet loss. In order to solve this the IETF defined extensions to Mobile IPv6 like Hierarchical Mobile IPv6 (HMIP [30]) or Fast Handovers for Mobile IPv6 (FMIP [31]) which optimize the time required to perform a handover, by introducing new elements on the infrastructure which can act as localized agents therefore reducing the time required to update the binding. On the Network Controlled mobility approach, the IETF is currently standardizing the Network based Localized Mobility management (NETLMM [32] [33]) protocol which based on ideas inherited from Mobile IPv6, allows the support of mobility in legacy terminals (terminals without MIPv6 support).
All these protocols could be used as the IP mobility management protocol. This thesis provides insightful details of the combined use of IEEE 802.21 and Mobile IPv6 although the knowledge acquired along this work is useful also if other IP mobility management protocols are used.

3.2 Bringing Ubiquitous Multihoming Support to the Internet

Multihoming is the ability of having different connections to Internet, potentially through different providers. As Internet evolves there are, at least, two different trends pushing the importance of multihoming:

- Internet communications are nowadays seen as strategic by companies and institutions. Reliability and degree of independence from particular service providers are an increasingly common requirement for these companies and institutions, and multihoming provided at the site level is the lever to achieve the mentioned objectives.

- There is a proliferation of access technologies everywhere. Therefore, it is increasingly common to have devices with several network interfaces (3G, WLAN, Ethernet and Bluetooth). To gain full advantage of robustness in communications and ubiquitous access by the ability of using the different accesses where they are available, a multihoming solution at the host level is required.

With these scenarios, it is expected that more and more multihoming situations will become common in the near future. As a consequence, a lot of work is being done in different Working Groups of the IETF to develop multihoming solutions that can provide the appropriate functionality while fulfilling requirements that guarantee that the solutions are deployable. There are several types of multihoming support, depending on the hierarchical position within Internet where multihoming wants to be provided [34]:

- Node Multihoming: Node or host multihoming means a node (host) with multiple interfaces that connects (potentially through different providers) to Internet. For instance, a laptop connected to Internet through an Ethernet and through a Wireless Access. Node multihoming can be viewed as a degenerate case of site multihoming, but it is of crucial relevance nowadays.

- Site Multihoming: Site multihoming refers to a stub network that connects to at least two different network service providers. These stub networks do not provide any transit service to other networks. Site multihoming potentially concerns a wide range of sites, from residential Internet users with two or three hosts, to very large enterprise networks composed of thousands of hosts.

- Multihoming of Small ISPs: Multihoming of small ISPs refers to ISPs that have a local presence, that provide transit services to stub networks, and that connect to multiple different upstream providers. Those small ISPs may be large enough to obtain their own provider-independent address space. They have their own AS numbers (ASNs), and use BGP [35] to advertise reachability information to other domains.

- Multihoming of Transit ISPs: Multihoming of transit ISPs refers to medium and large ISPs, that provide transit services to other ISPs and/or stub networks, and that connect to multiple upstream providers. They typically have more than a local presence, often a worldwide one. They always use their own provider-independent address space, and also use BGP to advertise reachability information to other domains. It is hoped that the number of those transit ISPs remains low, even in an IPv6 Internet.

From now on, we will focus on Node Multihoming since this is the relevant case for the work on this thesis.
The use of multihoming has several benefits such as redundancy, load sharing, performance increase, policy allowance or independence of the ISPs, although we will focus on the fault tolerance properties of the multihoming. By failure resilient we understand the ability of the node to resist (being able to continue the communication) on the case of several kinds of outages such as physical failure of a link, logical failure (misbehaving router interface), routing protocol failure, human errors or even transit provider failure.
To protect against the failure of a link, a multihoming solution must provide mechanisms to detect the link failure, explore alternative paths to the intended destinations, and re-home the traffic. A node is said to re-home when it is changing the provider that carries its packets, for instance because the link with the previous provider failed. This change should be as quick as possible. A required mechanism is to provide transparency for transport-layer sessions across such re-homing events. This means that the exchange of data between devices on the multihomed site and devices elsewhere on the Internet should proceed with no greater interruption than that associated with the transient packet loss during the re-homing event. Transport-layer sessions include protocols such as TCP, UDP and STCP over IP. Applications which communicate over raw IP and other network-layer protocols may also benefit from re-homing transparency. BGP is the most common way of enabling multihoming at site level used nowadays. Different mechanisms in BGP can be used to announce the address block of the site to each of the ISPs with different priorities, so one path (through one ISP) can be active and others (through other ISPs) can be used as backup. Several paths can be active at the same time by dividing the address space of the site in blocks, and announcing the blocks to the same ISP with different priorities, so one path can be active for an address block and a different one can be used for others. In any case, if the active path fails, BGP will update the routing tables of Internet core routers to use one of the alternative paths. The configuration of BGP announcements and path selection for outgoing traffic will usually be such that the outgoing and incoming traffic follows the same path. This mechanism is the most commonly used in practice for IPv4 multihoming, but nevertheless suffers from some limitations:

- It is not very flexible. It is well suited for an active/backup situation, but not for load balancing that can only be done per addresses and not per traffic load.
- Scalability concerns: If we announce different address blocks with different priorities to obtain some load balancing capabilities, different routes will be needed in the core routes for the address space of the site (one per address block with different path to follow). Even in the active/backup configuration we are overloading the BGP tables with different entries per address space of a multihomed site. As more sites are getting interest in obtaining multihoming capabilities this can become a serious problem. In fact this solution is currently suffering from more restrictive policies of the Regional Internet Registries (RIRs), typically allowing its application only to large sites.

So far, IPv4 has failed to provide a scalable solution to preserve established communications for arbitrarily small-size sites connected to the Internet through different providers after an outage occurs. In practice, the most common IPv4 multihoming solution, is based on the injection of BGP routes in order to make a prefix reachable through different paths, and it

would collapse if the number of managed routing entries would increase to accommodate small sites or even worst, individual hosts. On the other hand, the huge address space provided by IPv6 has enabled the configuration of public addresses from each of the providers of an end host. A step further has been taken in the SHIM6 WG [36] of the IETF to develop a framework to manage in an end-to-end fashion the use of the different addresses between a communication held by two hosts.

3.2.1 Multiple Care-of Addresses registration

In the current Mobile IP specification the MN can have multiple CoAs due to different active interfaces or multiple prefixes being advertised on the Visited Foreign Network, although only one of these CoAs, called the primary one, is registered with the Home Agent. Due to bandwidth, delay or cost considerations, it can be beneficial for a MN to be able to receive traffic through more than one interface/CoA at the same time. In order to allow this functionality in Mobile IP, the Multiple CoA registration extension is being defined by the IETF.
The operation of this extension is based in adding an identifier, called the Binding Unique Identification (BID), to each of the binding cache entries to accommodate multiple bindings. Each binding between a CoA and a HoA is identified by a unique BID which is notified to the HA and the CN by the Binding Update. By using this BID a MN can multihome the connection between the HA or the CN and benefit from the simultaneous use of several interfaces.
Although conceptually the use of the BID in the HA and the CN is similar, the operation of the nodes is quite different. The MN can register simultaneously several bindings with the HA by the use of a single Binding Update, this is called Bulk Registration. Bulk Registration is not allowed in the CN, since registering more than one address at the same time without performing the required security checks creates the same security considerations as the standard Route Optimization mechanism of plain Mobile IP. Nevertheless the MN can register multiple bindings in the CN one by one, performing a Return Routability process per CoA registered. Due to the magnitude of the number of Return Routability procedures to perform, a simplified version of it is allowed. In this simplified version, the home keygen token can be reused for each binding although the CoTI/CoT messages must be exchanged in a per CoA basis. As in the case of the Route Optimization Mode, the optimized binding between the MN and the CN has a limited validity of seven minutes.
Once a MN registers multiple CoAs on the HA or CN, every packet arriving from the MN can have different CoAs as source address. The HA or CN must check if the CoA in the packet corresponds to any of the CoAs registered on the binding cache and if it is not the case, drop the packet.
It is important to note that the Multiple CoA registration extension does not provide any mechanism to decide to/from which CoA the packets must be sent/received.
With multiple Care-of addresses registration, the mobile node gets multihoming capabilities, because applications are only aware of the Home Address, but in the network the different CoAs are used to address the packets. Moreover, some policies and priorities can be associated to a BID, which can be used to divide flows to multiple network interfaces by flow type, port number, or destination address.

If a Mobile Node has multiple bindings, fault tolerance can be provided by switching the binding in order to recover immediately from a link failure or a degradation of the path conditions. The node can detect a binding invalidation by packets loss or other protocols such as REAP (see section 3.2.3). When the Mobile Nodes moves, it may update the information regarding the new Care-of address obtained in the new network. The Mobile Node sends a Binding Update with the new Care-of Address and the corresponding BID. The receiver of the Binding Update, Home Agent or Correspondent Node, updates the binding entry which fits the BID provided by the Binding Unique Identifier sub-option in the Binding Update message. A Mobile Node can manage the mobility of each of the interfaces in a separate way by using a BID per interface.

3.2.2 SHIM6: Level 3 Multihoming Shim Protocol for IPv6

The SHIM6 [37] [38] protocol aims to provide multihoming functionalities by enabling locator agility below the transport protocols in order to offer failover and load sharing capabilities to the end nodes. A node located on a site which has multiple IPv6 prefixes uses the SHIM6 protocol to establish state with peer hosts, so this state can be used to provide failover to a different locator in the case the original locator stops working. Although the SHIM6 protocol is a host multihoming protocol in the sense that allows nodes located on a multihomed site to resume their communications after an outage, along this thesis it is used as a node multihoming protocol since it is used to handle different locators when the node is away from the site the locators belong to (see section 4.2 for more details). The protocol used by SHIM6 to detect failures and explore the available locators (REAP [39]) has been defined on the SHIM6 WG of the IETF, nevertheless the protocol itself is not part of SHIM6 and can be used in an independent way.
The main goals of the approach followed by SHIM6 to enable multihoming are the preservation of currently established communications in the presence of certain failure classes, transparency to upper layers in general and not requiring extra connection time to establish the needed state. This last goal is achieved by establishing the SHIM6 state once the connection has started and some packets are exchanged. The decision of securing a connection by SHIM6 is taken by an external heuristic.

The location of the SHIM6 shim layer within the IP stack is shown in figure 3.3. The SHIM6 layer is located between the IP routing sub-layer and the IP endpoint sub-layer. This allows the SHIM6 layer to be associated with an extension header which will be placed after any routing related extension headers of the packet. The location of the SHIM6 layer below the IP endpoint sub-layer allows SHIM6 to be used in conjunction with IPSec, fragmentation and destination options. The SHIM6 layer is also located below the Transport Layers. This allows the SHIM6 layer to provide Upper Layer Identifier (ULID) independence, but allowing the modification of the source and destination addresses of the packets, effectively modifying the path followed by the packets.
The state required by the SHIM6 layer is maintained per ULID pair, in particular all packets exchanged between two ULIDs are secured by a SHIM6 state. Mechanisms to allow the use of more than one locator pair at a time for a single ULID pair have been also defined, namely context forking. Figure 3.4 presents the SHIM6 protocol operation within each peer

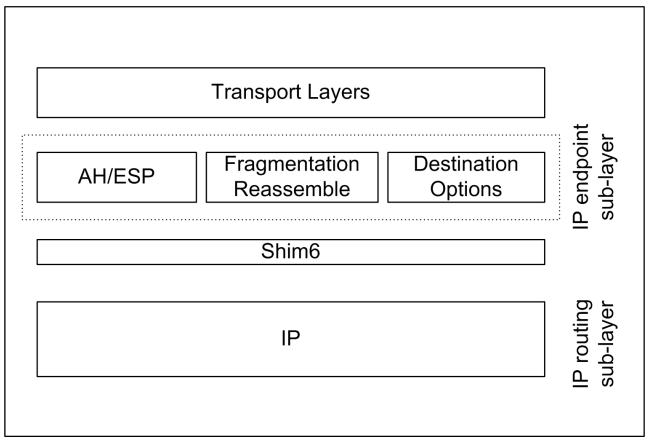


Figure 3.3: SHIM6 location on the protocol stack

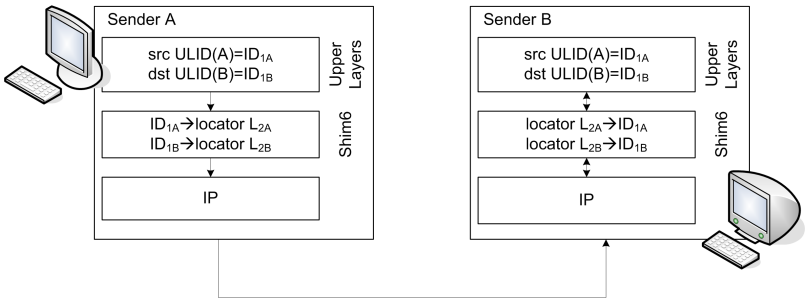


Figure 3.4: SHIM6 Operation

of a communication. Suppose two nodes (A and B) want to communicate. Each Upper Layer Protocol (ULP) selects an identifier following the rules presented in [40] and its extensions [41], and starts a normal communication through any transport protocol such as TCP or UDP. For this communication node A selects as ULID ID_{1A} and node B ID_{1B} [42]. This is called on SHIM6 the initial contact. Some heuristic on A or B determines that this communication is worth to secure through SHIM6 and starts a SHIM6 context establishment. At the end of the 4-way handshake required to setup a SHIM6 context, both nodes obtain a list of possible locators used by the peer. Since there is no problem on the communication, the exchange of packets continues without any intervention of the SHIM6 layer. In particular the packets are not modified and there is no extension header added to them.
At some point of time the path connecting both nodes is affected by a failure. The failure is detected by some mechanism, and an exploration of the available paths between both nodes is performed. One of the possible mechanisms to detect the failure is REAP, which is a protocol proposed to do failure detection and path exploration.
Once a valid path is found, it is notified to the SHIM6 layer which starts to rewrite the packets, modifying the source or/and the destination address (on the example, the ID_{1A} is rewritten by the locator L_{1A} and the ID_{1B} by the locator L_{1B}). The SHIM6 layer also adds an extension header to the packet on which a context tag is stored. This context tag is used as a key to find the appropriate SHIM6 context matching the packet so in reception the packet

can be restored to its original shape.

3.2.3 REAP: Failure Detection and Pair Exploration Protocol for IPv6 Multihoming

A fault tolerance solution requires a mechanism to timely detect failures across the communicating path, and a mechanism to discover a valid path after a failure. SHIM6 includes a component, named REAP (REAchability Protocol, [39]), to detect failures in any of the two unidirectional paths in use for a communication, and to explore different unidirectional paths to find a valid one after an outage. Note that REAP understands a bidirectional path as two unidirectional paths. The REAP instance of an endpoint for a given communication detects a failure if no packets are received for a given period of time. When a communication involves a bidirectional exchange of data at a sufficient rate, the determination of the availability of the path is performed without REAP-specific signaling. If only one of the parties is sending data regularly or the rate at which data is sent is too low, the REAP entities generate Keepalive messages to prevent the expiration of a timer at the other communicating node in the absence of failures. When no party sends upper layer data for some time REAP stops generating Keepalive messages and failure monitoring is no longer being performed. When a failure is detected, REAP triggers the path exploration component. The paths currently in use are first tested by sending REAP Probe messages. If this validation fails, different combinations of source/destination addresses are checked until a new pair of working addresses is found. Note that SHIM6 and REAP support the use of paths defined by different source and destination address pairs on each direction. A failure detection mechanism should require low resources to operate, and should waste little bandwidth for signaling purposes. The amount of state required for REAP operation, is three timers per communication and per endpoint. Additionally, it is quite efficient in terms of the number of protocol-specific messages exchanged since Keepalive messages are only sent for unidirectional communications or when the sending rate of data packets is too low. The low requirements exhibited by REAP make this protocol a good candidate for becoming the failure detection and path exploration mechanism of choice for other protocols requiring such functionality, such as HIP [43] [44] or Mobile IPv6 with registration of multiple CoAs [29]. Note that the failure detection component could be independently used for protocols requiring just this functionality. In this section we describe in detail the two components of REAP [39], the failure detection and the path exploration mechanisms. The failure detection mechanism of REAP is used to monitor the status of the pair of unidirectional paths in use for a communication. Note that although SHIM6 is able to manage different alternate paths for a communication, REAP only tests the pair of paths in use at a given time. To validate the current two unidirectional paths of a communication, REAP relies on two timers on each node, the Keepalive Timer and the Send Timer, and, when required, on the exchange of a message, named the Keepalive message. The Keepalive Timer is started each time a node receives a data packet from its peer, and stopped and reset each time the node sends a packet to the peer. When the Keepalive Timer expires, a Keepalive message is sent to the peer. Note that the reception of Keepalive messages does not modify the value of the Keepalive Timer at the receiving node. The Send Timer is started each time the node sends a packet, and stopped and reset each time the node receives a packet from the peer, either a data packet, or a Keepalive message.

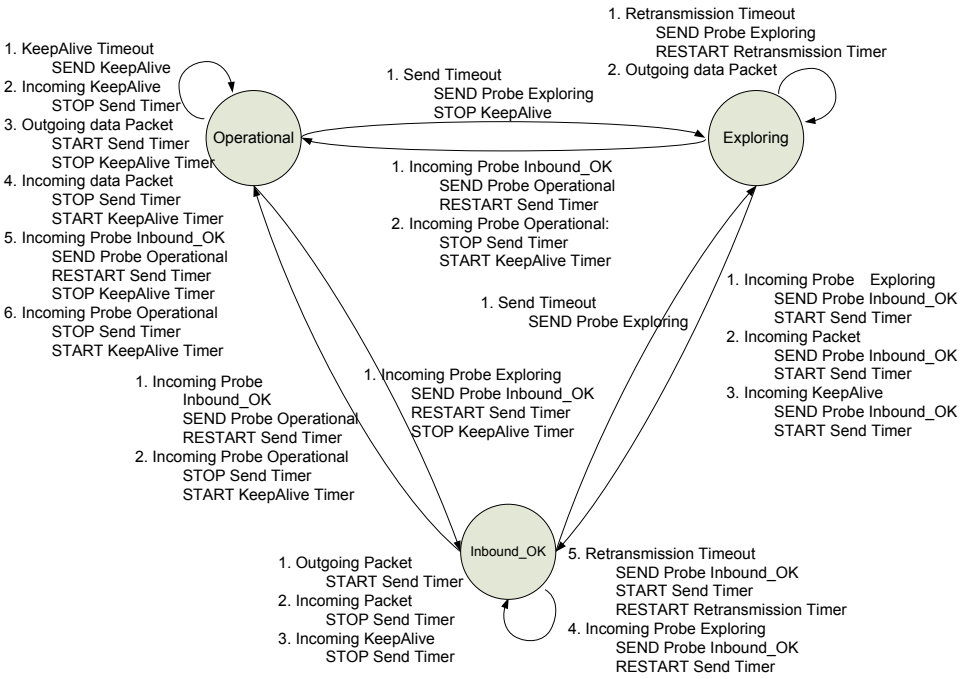


Figure 3.5: State Machine of REAP

If the Send Timer expires, i.e. no packet has been received during this period, a failure is assumed and the node starts the path exploration process.
The Send Timer expiration indicates that no return traffic was received for some time by a node that was sending data. On the other hand, the Keepalive Timer is used to assure that return traffic, in this case Keepalive messages, is generated in nodes that are receiving data but have no data to send. Note that the values of the Keepalive Timer and the Send Timer should allow at least one Keepalive message to arrive to the destination to avoid false failure reaction. The current specification suggests a default value of 10 seconds for the Send Timer, while no value is proposed for the Keepalive Timer. Note that neither experimental data nor analytical studies have been considered to propose the values for any of the timers that determine the performance of REAP. This was an important open point for the efficient use of the protocol in different situations that this thesis has addressed.
Once a node detects a failure, it starts the path exploration mechanism by changing its state from Operational to Exploring. First, a Probe Exploring message (a Probe message with the Exploring flag set) is sent to test the current address pair. If no response is obtained during a Retransmission Timer period, alternative outgoing paths, defined by different combinations of source and destination addresses, are tested sequentially by sending Probe Exploring messages and waiting for a Retransmission timer period. In the current specification, only one Probe is sent at a time. After sending four Probe Exploring messages, an exponential back off algorithm increases the Retransmission Timer. When a Probe Exploring is received, this means that a valid unidirectional path has been discovered for the incoming path. The node that has received the Probe Exploring message then changes its state to Inbound_OK and uses Probe Inbound_OK messages to continue exploring outgoing valid paths, and this type

of Probe messages include an indication of the valid incoming path. If the other node receives a Probe Inbound_OK, it can assume as valid the incoming path through which the packet was received, and it can obtain from the payload of the Probe Inbound_OK the valid outgoing path to be used. Then, the node changes its state to Operational, and sends a Probe Operational message in which it informs its peer about the validity of the path through which it received the Probe Inbound_OK message. A node that receives a Probe Operational message changes its state to Operational. It is worth to highlight that data is still being sent when the node is in the Exploring or the Inbound_OK states using the source and destination addresses in use when the node was in the Operational state. When the Operational state is reached again, the addresses in use are changed to the ones resulting from the exploration process. Note that these rules may lead to different state and message sending schedules: for example, one node can detect a failure and send a Probe Exploring that arrives at its peer before the peer detects a failure; or both nodes can detect a failure before receiving a Probe from the other endpoint. Figure 3.5 presents the state machine diagram that formalizes the behavior described above, including some transitions that occur only when a limited number of packets (either data, Keepalive or Probes) are lost, which could occur due to congestion.

3.3 Architectures for mobility and multihoming support

The concept of wireless heterogeneous overlay networks and vertical handovers can be traced back to 1996 with the early work performed by Randy H. Katz in Berkeley. In [45] the author presented a revised version of a paper published in 1994. This work explained the challenges in networking for the future years. One of these challenges was ”Allow a user to seamlessly move from his/her in-building infrastructure to the outside infrastructure to the in-building infrastructure of a client (or competitor) the user is calling on”. With this phrase, Katz expressed the need of allowing the user to roam between heterogeneous networks, while maintaining ongoing connections.
Early concepts of this overlay networks were also presented in [46] and [47]. At the time the test bed used in this work was formed by state of the art wireless technologies including WaveLAN, Infrared and Ricochet wireless networks. These studies were the first ones introducing the vertical handover concept, letting the users of this test bed to roam between different wireless technologies. The authors also recognized during these works the requirements in order to realize seamless handover in heterogeneous environments, being among these requirements the need of a global network management functionality. It is interesting to note how in [47] the authors reached to the conclusion that the predominant component on the delay of a vertical handover is the time required for a Mobile Node to detect that it has moved into or out of a wireless overlay. One of the main contributions of IEEE 802.21 is the use of information services and link layer triggers to improve the time needed to detect a new network.
Through the years several research projects have studied integrated network architectures formed by the overlapping of different technologies. Major projects like BRAIN/MIND [48], WINE/GLASS [49], MIRAI [50] and FIT-MIP [51] have all assumed a similar All-IP based architecture. The key element of this architecture is the Point of Attachment (PoA) to the network. In this architecture the PoA is an IP enabled intelligent port which provides the basic access in each access network. All management decisions are

taken by these intelligent ports while the mobility management, QoS brokering or capacity handling is performed by different entities located on the network.
At this early stage all the IP mobility research efforts were focused on understanding the performance issues of the IP mobility protocol available at the time, Mobile IPv4. Works such as [52] or [53], focused on understanding the performance issues and evaluating the handover performance of Mobile IPv4.
Later on, with the appearance of Mobile IPv6, test beds incorporating new technologies were deployed. These deployments were focused on horizontal handovers, trying to decrease the delay while performing a handover and studying the influence of such handovers on transport protocols such as TCP. In these works the first performance analysis of the Internet protocols used over cellular links such as GPRS were performed. An example of this kind of work is [54] where the authors present a detailed analysis of the properties of a GPRS channel, studying the effect of this properties in TCP.
After the horizontal handover concept was studied, the research community efforts moved to understand the challenges arising by the upcoming 4G architectures. One of these challenges was the heterogeneity of the radio access networks. 4G architectures are characterized by the use of several different technologies as radio access networks which attach in a flat way to the IP core network. Works describing the requirements and design decisions regarding these new architectures appeared, such as [55], in which the authors present an exhaustive analysis of the problems of vertical handovers. This work presents a tutorial on design and performance issues for vertical handover on a 4G heterogeneous network, focusing on design decisions such as the IP mobility management protocol to use, the handover decision metric, policy design, Mobile Initiated handover (MIHO) vs. Network Initiated handover (NIHO), radio link transfer or context transfer. Works focused on terminal architectures and requirements for efficient vertical handovers can be found on [56] and [57]. In this last work the authors introduced media-dependant Link Layer events which are generated and treated to decide whether to perform a handover or not. The main difference with the IEEE 802.21 approach lies on the use of media independent link layer events and triggers [58] which are then processed by an external algorithm (this algorithm corresponds to a MIH user) allowing the development of algorithms able to handle the heterogeneity without the need of handling the specifics of each technology. The specifics of such algorithms or the proper configuration of the triggers generating the events used on the algorithms are some of the aspects the specification does not cover and need further study.
In the recent past, network architectures using heterogeneous access networks have been further studied by the deployment of several test beds exploring these concepts. Reference [59] presents the LCE-CL test bed which was a MIPv6-based test bed used to study the integration of different radio access technologies into one loosely-coupled IP-based core infrastructure. This test bed was mainly used to understand the performance issues of the vertical handovers, on [60] the authors perform experimental measures with this test bed, integrating several technologies. The authors focused on understanding the issues involved on transmitting TCP traffic while performing handovers between these two technologies, presenting also some possible solutions and architecture changes which may mitigate the effect of the issues discovered. This test bed managed the heterogeneity of the networks without any adaptation layer nor network intelligence, basically performing experiments

testing Mobile IPv6 handover performance between different technologies without adding any support neither on the terminal nor in the network.
A more recent example, Moby Dick [61] [62] [63] proposed and implemented a global end-to-end MIPv6-based architecture to offer QoS in heterogeneous environments. The test bed included UMTS-like [64] TD-CDMA wireless access technology, IEEE 802.11b WLANs, and wired connectivity. The mobility control in the Moby Dick architecture was layer 3 based, and no interaction with layer 2 technologies for efficient handover management was studied.
The work presented on this thesis have been partially funded by the Daidalos project [65] [66]. The architecture designed by this project allows for media independent handovers, triggered either by the MN or the network, supporting optimized mobility and resource management [67]. The Daidalos architecture presents the trends of the future communication architectures, focused on all-IP cores with heterogeneous access technologies.
In this context the IEEE 802.21 specification has been developed. Currently the use of this specification to improve the performance of vertical handovers and as an enabler for the tighter integration of different radio access technologies with the core of the network is a hot topic of research. Recent works in the mobility research area started to use this specification as a way of improving the performance of the handover. References [68] and [69] present the first experimental evaluations of the use of IEEE 802.21. In these works the authors study the handover latency and the packet loss of a mobility architecture based on SIP and FMIP using IEEE 802.21 to decrease the discovery time of the new PoA. In these architectures the MN is able to gather information of the target network via IEEE 802.21, decreasing the total time needed to perform a handover. This is an example of how a clever utilization of the information services of IEEE 802.21 can be used to improve the performance of MN's operations, in this case the reduction is focused on eliminating the time needed to discover the movement and configure the L3. These works take advantage of the 802.21 capabilities to discover neighbor networks and the characteristics of them. Although these works used 802.21 to improve the performance of the handovers, they do not take full advantage of the possibilities of the technology, being 802.21 used mainly for information purposes only not being completely integrated on the network architecture. In order to use the full capabilities of the 802.21 technology, it is needed to use the information services offered by 802.21 but it is also fundamental to be able to gather dynamic information such as network availability, signal levels or even network generated events. Hence a detailed analysis of the proper configuration of the 802.21 link layer triggers to perform seamless handover is required.
Although most of the efforts in the IP mobility research area have been focused on solutions were the mobility is managed by the Mobile Node (Mobile Initiated Handover), another issue that this thesis addresses is the coordinated operation of the network and terminal to improve the mobility management (Network Controlled Handovers), hence the final user experience. Network Controlled handovers (NCHO) are different from Network Initiated Handovers (NIHO). When using NIHO the network decides where and when the handover is performed. The NCHO paradigm implies that the network has the final decision to accept a handover, although the handover can be mobile initiated or network initiated, or even both possibilities can be combined in a network, where the use of each one depends on the situation.

Network Controlled handovers for 4G networks have been previously studied on the literature. On the 4G networks an all-IP core is directly connected to the radio access, which can be of different technologies. In [70] the authors discuss how to distribute radio resource management in a multi-radio access network, related with 4G architectures. They identified three main distribution strategies, namely network centralized, network distributed, and radio resource management performed by the terminal. They conclude this work by suggesting a hybrid architecture based on distributed network management and terminal driven, mapping it to the LTE (Long Term Evolution) architecture defined by the 3GPP. Other work defining a 4G architecture where NCHO is used can be found in [71]. This work describes the IP2 Mobility Management Protocol specifically designed to satisfy mobile operator's requirements for next-generation mobile networks. IP2MM exploits the network controlled approach instead of a terminal controlled mobility management. The main conclusion is that with this type of protocols a better performance of the network can be achieved. However the paper mainly focuses on the performance in mobility control and packet throughput, not performing an analysis of the overall performance gain.
The Network initiated handover concept has also been largely studied on the literature although the research was more focused in radio resource management for cellular networks. In [72] a formulation of the radio resource management problem is provided. This work presents a survey of the current trends on techniques to deal with radio resources, mainly it presents three types of techniques, waveform, access port and transmitter power. By using the waveforms (frequencies or orthogonal codes) the users are allocated to different signal types minimizing the interference between them. By access port the authors named the base stations, basically another resource management technique is to move users from one base station to another with less interference or more free resources. Finally by adjusting the transmission power the global interference of the system is reduced. The access port technique, allowing the network to move users from heavily loaded base stations (BSSs or APs) to less loaded ones increasing the resource utilization of the system, is a good candidate as a technology to be used in heterogeneous systems were the different characteristics of the networks can be used to provide flexibility to the architecture, which then is able to adapt to different scenarios or user profiles. Although this technique has been for a long time used on the mobile telephony systems, a deep study of the implications of applying these ideas to an heterogeneous scenario is needed, taking into account the specifics of such scenarios were different technologies may be used, with different ranges, transmission power and bandwidths.
In [73] the authors present a centralized or common Radio Resource Management system to deal with the management of heterogeneous networks on the same area. Their approach is to handle the resource management on a central entity which is able to decide which users should be moved to other technologies in order to improve the overall efficiency of the system. In this work the authors perform some simulations to prove that the use of a central entity managing the mobility can improve the overall performance of the network by assigning users to different base stations in function of the system's load. A similar approach is presented in [74]. Although the architectures presented in these works show the benefits of using some kind of network management of the users, in order to deploy a network controlled mobility system in the future networks further steps are required. In first place Mobile IP as the protocol managing the mobility must be incorporated, providing an

architecture which integrates the capability of resource management on the 802.21 reference model. In this integrated architecture, the information about the system must be accessible by the central management system. IEEE 802.21 allows the central entity in charge of the resource management to get information related to the signal level being measured by the nodes, information about the topology of the network, available resources etc. which is not available in other scenarios, although the mechanisms to transport this information and an analysis of the specific information required or the algorithms to react upon it, are not defined. The use of such network initiated architecture also requires the modification of the trigger mechanisms which now must provide information to the network regarding the current conditions of the terminal and the surrounding networks, being the terminal also able to react upon events or commands generated by the network.
The use of Network Controlled Handovers (NCHO) as a way to improve the mobility performance has been also studied. In [75] the authors present a network controlled handover architecture used to improve the handover delay. The results presented prove that the use of this approach reduces the time needed to perform a handover. The proposed architecture assumes the existence of communication path between the MNs, APs and a central entity which is able to command the handovers although this communication is not 802.21 based. In this work the main NIHO related philosophy of IEEE 802.21 are envisioned, although with limited scope.
Finally, in the research community, a number of approaches aiming at providing network support for mobility management have been proposed and examples are [76] [77] [78]. However, both network and terminal handover optimization schemes for heterogeneous networks, framed under a common set of functional components and associated protocol operations, are not yet accurately addressed and evaluated.
The third important topic of this thesis corresponds to the multihoming support in the terminals of the future Internet. Reference [79] presents a survey of current and future mechanisms to support multihoming. In this article the authors identified SHIM6 as one of the most promising protocols to provide multihoming support at host level. The combination of SHIM6 and Mobile IPv6 for mobility and multihoming support has also been proposed [80] [81], although the architectures presented on these works do not define how path failure and exploration is done.
The protocol being used by SHIM6 to detect path outages and recover the communication from them is REAP, but this protocol is a recent proposal and there is a lack of understanding of its configuration and performance. In [82] the authors present an experimental evaluation of only the path exploration part of the REAP protocol. They validate and obtain measurements related with the performance of the protocol with concurrent path exploration. In order to take full advantage of REAP an analysis of the failure detection part of this protocol is also required.

3.4 Summary and Open Issues

Along this chapter we have provided an overview of the protocols used as building blocks to form architectures providing multihoming and mobility across heterogeneous technologies. We have also given an overview of relevant works on the literature which tried

to solve, at least partially, the problematic addressed in this thesis. We started providing a vision of the protocol used to handle mobility, Mobile IPv6, providing its basic functionality description. In a second stage we have presented an overview of two protocols providing multihoming support, Multiple Care-of Address Registration Extension for Mobile IPv6 and the SHIM6 protocol. The Multiple Care-of Address Registration Extension for Mobile IPv6 protocol allows the terminal to register multiple addresses with its Home Agent and Correspondent Node, therefore allowing the multihome of the Mobile Node's point of attachment to the Internet. SHIM6 is a protocol that allows the decoupling of the identifier and locator role of the IP address, allowing the modification of it without impacting upper layers. The use of this protocol allows a node to multihome its Internet access but it does not provide mobility support.
Once a node has multihoming capabilities, in order to be able to take advantage of this capabilities, it is required to have a mechanisms to detect and recover from failures on the path. We have selected and explained a protocol called REAP which enables the failure detection and path exploration on the terminal.
Through the explanation of these building blocks and the proposals which can be found on the literature several open points have been identified. In first place, a study of how a mobile node can take full advantage of the capabilities provided by IEEE 802.21 is required, focusing on the use of the information provided by the network and the use of link layer triggers. The configuration of the link layer triggers and the effect of the terminal's speed on it must be also analyzed. Secondly it is needed to analyze how to introduce the Network Controlled mobility capabilities on an heterogeneous network, taking into account the possibilities opened by IEEE 802.21. By the use of the informational capabilities of IEEE 802.21 the network can implement sophisticated algorithms based on information available at network and terminal level, reaching new limits on network performance. Finally to allow the terminal to detect failures and recover from them, a detailed study of the REAP's behavior, providing exact figures which allow the perfect configuration of its parameters, is required.

Part II

Architecture Definition

Chapter 4

Architecture

On this chapter details about the architecture used along this thesis are provided. First an analysis of the functionality required for the characteristics of the architecture is performed. Secondly an architecture complying with the functional requirements is proposed.

4.1 Functional Requirements

This thesis foresees a future where the operators will handle several technologies on their access networks. In this future, there are not 3G only operators, as an example, instead operators will provide communication services across a set of access technologies among which the clients and the network can select the preferred one. This future opens the paradigm of heterogeneous networks and multihoming devices, which can take advantage of the diversity to increase their bandwidth, reliability, etc.
Another important characteristic of this scenario is the mobility. Operators will have to provide mobility on an environment with higher complexity as the mobile nodes became multihomed and the mobility must be supported across several different technologies and administrative domains.
The current trend in the evolution of operators' networks is to architectures based in an IP core and several access technologies. These networks will offer all kind of services including voice, video and data services such as web browsing, P2P, etc. The use of different access networks is required to support the heterogeneity of services offered or envisaged nowadays. From the point of view of the services, a single technology cannot efficiently support different requirements in terms of delay, number of users, mobility, etc. From the point of view of scenarios, a single technology cannot efficiently provide access in different situations of density of users, type of traffic, etc. In such scenarios it is required to adapt the Internet paradigm, focused on the end user, allowing the operators to have some control over the use of the network. For this future to became a reality the functionalities in the network and/or the terminals must at least support:

- IP Mobility. Users must be able to roam or handover between different technologies and operators.
- Mechanisms for the efficient use of the network resources in environments with strong user concentration and mobility.

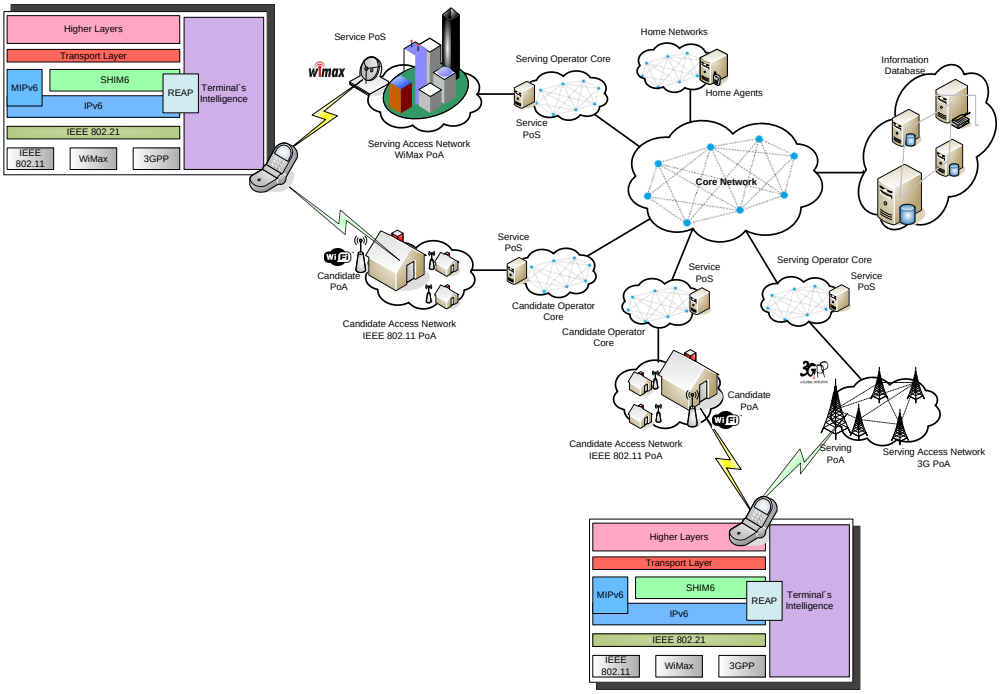


Figure 4.1: General Architecture

- Multi-technology smart terminals, able to handle multiple interfaces at the same time, gaining advantage of the use of multihoming and able to handle their own mobility.

Taking into account the requirements defined above, in the next section, a network and Mobile node architecture is presented.

4.2 Proposed Architecture

Figure 4.1 presents the general architecture proposed in this thesis. It relies on three building blocks. The first block corresponds to the IEEE 802.21 technology which allows a MN to handover between heterogeneous IEEE 802 and cellular technologies. The second building block corresponds to protocols which allow IP mobility. In this work, we suppose all nodes use Mobile IPv6 to handle IP mobility although optimizations of it or other protocols can be incorporated without impacting the concepts studied. Finally the third block provides end to end multihoming support, we assume the use of SHIM6 and the failure detection protocol built on top of it, REAP. In the following lines we draw a complete description of the architecture which complies with the requirements defined in section 4.1.

4.2.1 Network Architecture

Figure 4.1 shows a core network formed by several operators whose access networks are based on different technologies. In this particular example, the available access networks are built on IEEE 802.11 (WiFi), IEEE 802.16 (WiMax) and 3GPP technologies. In order

to provide mobility across heterogeneous technologies, IEEE 802.21 has been chosen. This requires the network to support it, basically by adding intelligence to the network. An IEEE 802.21 network is composed by Points of Attachment (PoAs), Points of Service (PoSs) and Information Services. The Points of Attachment must be modified in order to understand IEEE 802.21 signaling so they are able to provide information to the network and the mobile nodes. The Points of Services are in charge of handling all the required processes for a handover. Finally the Information Services are used to provide static information related with the network on a geographical area. Operators in order to take full advantage of IEEE 802.21 technology should sign agreements between them, allowing the use and sharing of information regarding their networks. As previously stated, this thesis assumes the use of Mobile IPv6 as the IP mobility management protocol. Mobile IPv6 requires some infrastructure in the network in order to work. Basically each Mobile Node belongs to a Home Network, the IP address used while staying in the Home Network is called Home Address (HoA). This address is used as an identifier when the Mobile Node changes its point of attachment to the network. Packets sent to the Mobile Node by any Correspondent Node, are sent to the Home Address. Once the packets arrive at the Home Network, there is an entity called Home Agent which is in charge of forwarding the packets to the current location of the Mobile Node. Route optimization allows to move the communication to a direct $CN \leftrightarrow MN$ path. On the architecture presented on figure 4.1 we assume the Home Network of the Mobile Node belongs to an operator, which maintains this network private. A Mobile Node belonging to an operator obtains a Home Address, remaining always in a Visited Network. The infrastructure needed by Mobile IPv6 is provided by the operator, which adds the servers acting as Home Agents, and provides the Home Address to each Mobile Node belonging to it.

4.2.2 Mobile Node Architecture

Figure 4.1 also presents the protocol stack of the Mobile Nodes used in the architecture. The physical layer, presents a multihomed device, with several physical and MAC layers. Above the physical layer, the IEEE 802.21 layer takes care of managing the control plane related to the multiple interfaces, abstracting the higher layers of the technology diversity. On top of it the IPv6 layer is in charge of internetworking being Mobile IPv6 a part of it. On top of the IPv6 layer the SHIM6 layer provides the transport protocol with an identifier which does not change even if the underlying IP address changes and so supporting the multihoming functionality. This protocol stack assures the continuity of the communication across movements and provides reliability through multihoming.
Mobile IPv6 is a mobility oriented protocol, not providing any support for multihoming. Related work, such as the Multiple Care-of address registration [29], tries to include multihoming support on IPv6 by the use of multiple Bindings on the HA and the Correspondent node. Although these efforts are useful to provide certain bandwidth increase or control over flows they do not provide full failure tolerance. Figure 4.2 presents the reference scenario for Mobile IP utilization for a communication between two Mobile Nodes with and without Route Optimization. Each of the nodes has a Home Address (HoA_1, HoA_2) and a Care of Address (CoA_1,CoA_2). Mobile IP can operate in two modes, Tunnel Mode and Route Optimization Mode. On the first case, all packets exchanged are routed through the Home

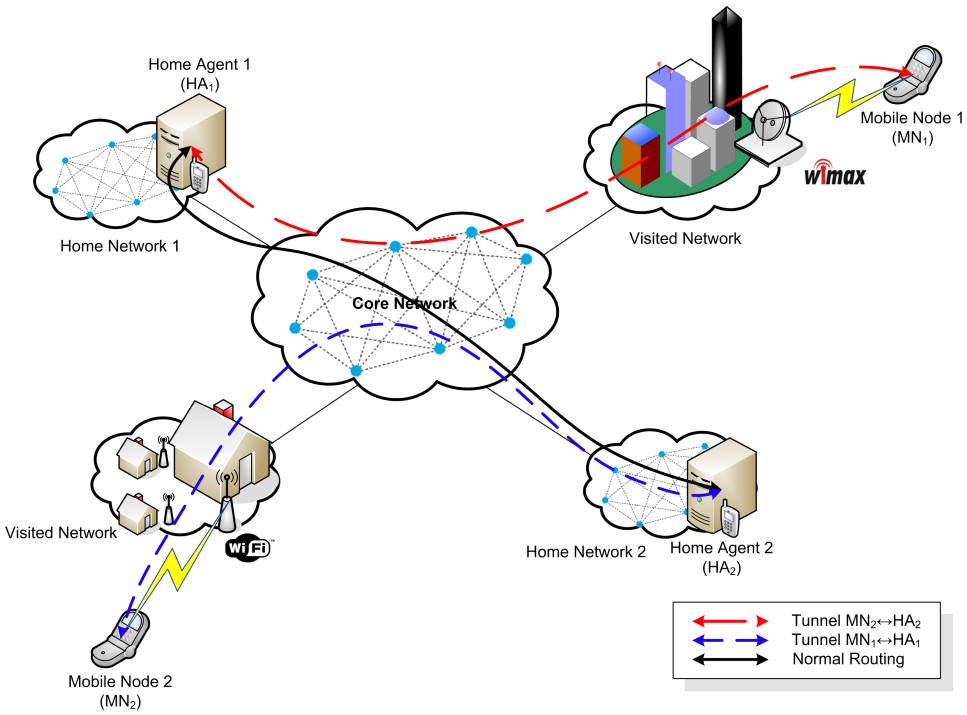


Figure 4.2: Mobile IP Scenario

Agent. In Route Optimization Mode the packets are exchanged directly between both nodes although some signaling is exchanged through the Home Agents for security reasons.
A packet sent by the Mobile Node 1 to Mobile Node 2 (IP source address HoA_1, IP destination address HoA_2) in Tunnel Mode is first encapsulated into an IP packet with IP source address CoA_1 and IP destination address HA_1. At reception the Home Agent (HA_1) decapsulates it and sends it to HoA_1 following the standard routing paradigm. The Home Agent (HA_2) captures the packet when it arrives to the Home Network of the Mobile Node 2. The packet is then encapsulated into an IP packet with IP source address HA_2 and destination address CoA_2. At reception of the tunneled packet, the Mobile Node 2 decapsulates the packet and forwards it to the IP stack.
If Route Optimization is used, the packets are exchanged directly between both Mobile Nodes, using a routing header type 2 as explained on section 3.1.1. The signaling required to maintain the binding between both Mobile Nodes is exchanged through the Home Agents. Focusing on the communication in Tunnel Mode, the path followed by a packet can be divided in three parts:

- Path $CoA_1 \rightarrow HA_1$.
- Path $HA_1 \rightarrow HA_2$.
- Path $HA_2 \rightarrow CoA_2$.

A failure in any of these three paths has as consequence the interruption of the communication between the Mobile Nodes.

Taking into account the possibility of using Route Optimization between the nodes, another path must be considered. This path is CoA_1 →CoA_2. A failure on this path interrupts the communication, although if the three paths involved on the Tunnel Mode are working, the communication can be recovered.
In order to provide failure recovery capabilities by the use of multihoming to a Mobile IP based communication, we propose the use of the Multiple CoA Registration (MONAMI6) extension to Mobile IPv6 in joined operation with SHIM6. The use of MONAMI6 allows the registration of multiple CoAs between the Mobile Node, the Home Agent and the Correspondent Node. By the use of multiple CoAs a failure on the path between a CoA and a HA can be overridden by the rerouting of the packets through a new CoA.
The use of SHIM6 associated to the different HoAs allows the modification of the Home Addresses used on the ongoing communication. By modifying the Home Address used another Home Agent is selected, this allows the recovery of the communication in the case of failure on a path between Home Agents or failure of the Home Agent itself.
The REAP protocol is used in this architecture to detect the failure of the path in use. In the proposed architecture the REAP protocol does not form part of SHIM6, being designed as a cross-layer protocol which knows the addresses used by SHIM6 to establish its context and having access to the Binding Cache of Mobile IPv6 and the information regarding the interfaces through which the packets are being sent and received. On all cases REAP monitors the validity of the bidirectional path HoA_{Ax} to HoA_{By}.
On the following lines an example of the joined utilization of all these protocols is provided. Suppose two nodes (A and B) want to communicate. Node A has several HoAs (HoA_{A1}..HoA_{An}) depending on the number of interfaces, ISPs and the number of Home Addresses provided by each ISP. While moving it acquires several CoAs (CoA_{A1}..CoA_{An}), depending on the number of active interfaces and number of IP addresses provided on the Visited Network. The same occurs with node B. Figure 4.3 presents the reference scenarios for this example supposing each MN has two active interfaces and two Home Addresses.

After both nodes are established in a Visited Network, for robustness or load sharing each node performs a multiple CoA registration between the Mobile Node and the Home Agent and, if desired, between both Mobile Nodes (performing at least one complete Return Routability procedure and a CoT/CoTI exchange per CoA registered between each MN and the other MN). This can be performed for all Home Agents or the binding can be done when it is needed.
Following the multiple CoA registration a SHIM6 context is established. The addresses taken into account for the SHIM6 context establishment are the available Home Addresses of both nodes.
For the time being we will focus on the scenario without Route Optimization. In this scenario each of the nodes has the following configuration at this point. The identifier seen by the upper layers corresponds to one of the Home Addresses originally selected for the establishment of the connection, we will suppose these Home Addresses are HoA_{A1} for MN A and HoA_{B1} for MN B. The SHIM6 context has been established taking into account all possible Home Addresses, so the SHIM6 context can be defined as $SHIM6\{(HoA_{A1}, HoA_{A2}), (HoA_{B1}, HoA_{B2})\}$. Mobile IP is assumed to be using MONAMI6 and each of the CoAs is registered with every HoA. For the MN A, this means there are two bindings established per HoA, one with CoA_{A1} and other with CoA_{A2}.

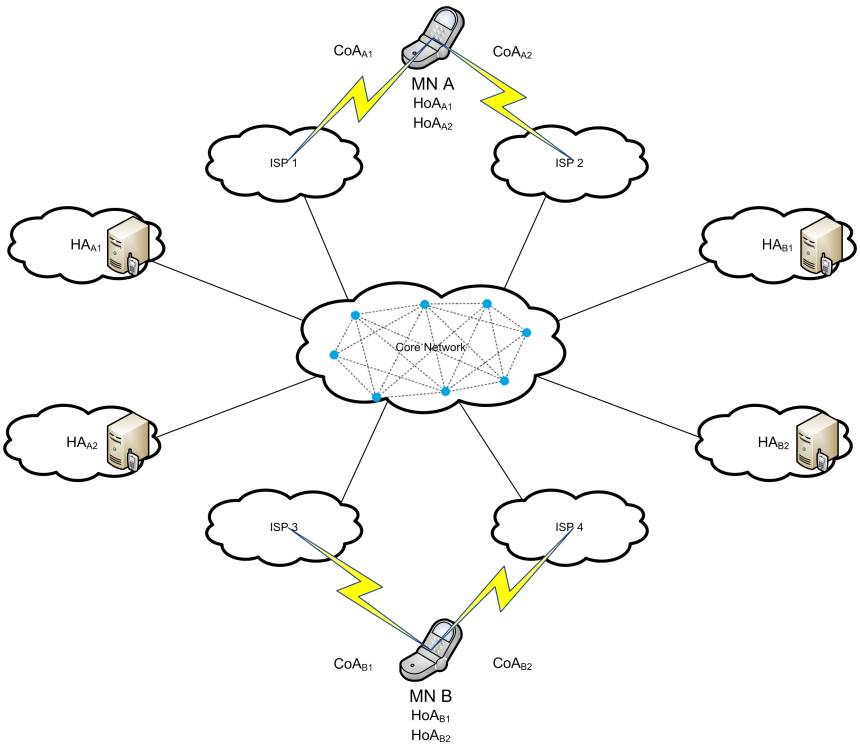


Figure 4.3: Multiple CoAs Scenario

On the other hand, REAP is monitoring the path between both nodes, as the communication has been established between HoA_{A1} and HoA_{B1}, this is the path currently being monitored by REAP, but note that this translates to monitor the path in use $CoA_{A1} \leftrightarrow HoA_{A1} \leftrightarrow HoA_{B1} \leftrightarrow CoA_{B1}$.

After a time, the current path is affected by an outage. This failure can be detected by the use of REAP or either by a link layer trigger. It is important to note the different timing of these two detection mechanisms. REAP relies on the monitoring of the packets flowing through a certain path and on timers to detect the failure. Through the use of REAP, a failure affecting the complete path traversed by the packets can be detected, although the time scale of this detection can be long (see chapter 7). In the other hand, by the use of IEEE 802.21, the physical layer can detect and notify higher layers of the failure or abnormal behavior of the access link. By the use of link layer information, the failure of a local link can be detected in a time scale of milliseconds although this information is related to local events, not being able to detect failures in parts of the network not directly connected to the MN.

Once a failure is detected, the path exploration mechanism of REAP is started. This action is performed in parallel, although with some time difference, on both sides of the communication, since REAP is running in both nodes. At this moment REAP starts sending Probe messages through the different possible paths in order to find an available path through which resume the communication. Following the normal behavior of REAP, the first Probe message is sent through the path currently in use, in order to check if there is a real problem or it is a false positive. Regarding the sending of the Probe messages, in order to check if all

the paths connecting the HA to the MN are working, the MN must sent the Probe messages through all the bindings established with the HA, so in this case REAP performs a parallel exploration of all paths connecting to the peer through the originating HoA. This Probe messages reach the HA which forwards them to the MN.
In our network design we have introduced a modification to the Home Agent in order to take full advantage of the functionality provided by REAP. When a Home Agent receives a REAP Probe message destined to a MN to which the Home Agent has multiple bindings, it forwards the Probe message through all the bindings at the same time. Through this mechanism the MN receives the Probe message indicating the other side has detected a problem in the communication, even if some of the bindings do not work. The multiple reception of the Probe message through all the interfaces has a second purpose. In case the problem is affecting one (or several but not all) of the interfaces (or addresses) through which the MN attaches to the network, the MN will detect it because the Probe is being received only through a sub set of these interfaces (or addresses). In case the MN receives some of the Probe messages sent by the peer, the failure is located in some point between the HA and the MN. As the Probe message has been received, one or more of the interfaces used to communicate with the HA is working. Then the MN deregister the CoAs which are known to be not available and the communication can be resumed through the new ones.
We have also introduced another modification to the standard protocol stack, in order REAP to reach a stable state when a failure occurs. In the current specification, the Probe messages carry information regarding the addresses through which Probe messages have been sent along with information regarding the addresses from which Probe messages have been received. This information is used by the REAP algorithm to decide which address pair use to resume the communication. In our architecture the information sent into the Probe messages regarding the address used to send the Probe messages must include the CoAs, not the Home Addresses.
On the other hand, if the MN does not receive any Probe message, the communication cannot be resumed using this HoA. Both peers, following the REAP's state machine, wait for a certain time to check if the current path is working and after this time REAP checks possible alternative paths. As the SHIM6 context is established taking into account all the HoAs, REAP starts checking possible available paths between the HoAs, until a new pair of HoAs is selected to be used. Then the SHIM6 layer modifies the packets delivered by the higher layers with the new source and destination Home Addresses, which are routed by Mobile IPv6 to the appropriate Home Agents and destination CoAs. On reception, the SHIM6 layer modifies the packets, rewriting the original IP addresses configuration on the header and delivering it to the higher layers.
In the case of Route Optimization being used, the external protocol can detect the failure also by a failure on the Return Routability procedure. If Route Optimization is used, the communication can be flowing through the optimized path but a failure on the path through the Home Agent may lead to a generalized failure on the communication due to the MN not being able to perform the Return Routability procedure required to maintain the optimized path.
Suppose the previous scenario but using Route Optimization. The scenario configuration is the same as without Route Optimization, except that both MNs have performed at least one Return Routability procedure and are using an optimized path, which we suppose is

using directly CoA_{A1} and CoA_{B1}. In this scenario a failure can be detected through three means, via Link Layer events, Return Routability procedure failure and REAP. If the Return Routability procedure fails, Mobile IP will move the traffic from the optimized route to the tunnel route. The Return Routability procedure can fail due to a failure in the direct path between both MNs or the path going through the HA. In the case the failure occurs on the direct path between the MNs, is very probable that REAP detects the failure before the Return Routability procedure is started. In the other hand if the failure affects the path going through the HA, REAP is not able to detect it. After a period of time, Mobile IP redirects the optimized flow back to the path through the Home Agent. At this point, REAP detects the failure and proceeds the same as before.
To increase performance, our architecture schedules the Return Routability procedure in such a way that a failure of the not optimized path is detected, by a failure in a Return Routability procedure, before the expiration time of the optimized path. Once the failure through this path is detected, REAP performs an exploration of the paths similar to the one explained in the case without optimization. If the optimized path is still working because the failure is only affecting the non-optimized path, once the exploration procedure finds an available path a Return Routability procedure can be performed using the new path to send the HoT/HoTi so the optimized path does not need to be cancelled.
On the other hand if the failure affects the optimized path, REAP is able to detect it, triggering an exploration. Once a path is found, and if the external algorithm considers that an optimized path must be found, another exploration taking into account only direct connections between both MNs is performed to ensure that the final new path selected is able to be optimized.

4.3 Summary

This chapter has been devoted to present the architecture proposed by the author in this thesis. The architecture provides to the Mobile Node and the Network with control mechanisms to handle mobility in heterogeneous environments and proposes a protocol stack allowing the terminals to benefit from multihoming.
In the following chapters, we discuss in detail each one of the building blocks of the architecture. Note that although these blocks have been presented within a common framework to form the proposed architecture, each of the mechanisms presented in this thesis has its own independent value. Following this reasoning, chapter 5 analyzes the Mobile Initiated handover paradigm in the framework of IEEE 802.21. Chapter 6 analyzes the Network Controlled handover concept, identifying the benefits of including it in the IP networks and proposing a possible integration in the IEEE 802.21 framework. Finally chapter 7 focuses in the analysis of the REAP protocol and its interactions with higher layer protocols, in particular TCP.

Part III

Mobile Initiated Handovers

Chapter 5

IEEE 802.21 enabled mobile terminals for optimized WLAN/3G handovers

5.1 Introduction

The IEEE 802.21 Working Group (see chapter 2) is specifying a method to provide enhanced vertical handover mechanisms across the 802.x and the 3GPP/3GPP2 family of networks and defining internetworking functionalities. The 802.21 solution is based on a 2.5 control middleware (the Media Independent Handover Function, MIHF) that abstracts layer-2 specific characteristics to upper layers (namely layer-3). Thus, IP based protocols are provided with a method to control the underlying technologies by means of a set of appropriate SAPs (Service Access Points). For example, a variety of parameters useful for selecting a handover target are defined in an abstract way, and the levels above layer-2 only need to deal with these abstract parameters.

This chapter is devoted to analyzing the integration of the upcoming IEEE 802.21 standard in a terminal centric architecture using Mobile IPv6 as IP mobility management protocol, (see chapter 3). The IEEE 802.21 work provides a useful framework to efficiently implement solutions for inter-technology seamless handovers and internetworking, but concrete solutions are out of its scope: 802.21 does neither specify which parameters should be taken into account nor how those parameters should be used. Thus this chapter is focused on understanding the relationship between all the elements needed to provide mobile initiated heterogeneous seamless handovers, providing conclusions regarding the required information, modifications to the current protocols and configuration guidelines.

The mixed WLAN-3G environment is going to be an important and widespread case in the near future and it is the focus of this chapter. Existing solutions for handover decision in WLAN environments have been based mainly on signal level. Considering scenarios in which a terminal can freely move across 3G and WLAN coverage cells, the configuration of the terminal for network detection (e.g. WLAN signal level detection) and attachment is

a critical issue. For instance, a user preferring WLAN connectivity (when available) over 3G may need a threshold configuration different from a user preferring 3G. IEEE 802.21 provides a method to configure (upon events or timers) specific thresholds for vertical handovers between 3G and WLAN, the handover algorithm configures the power thresholds, and then handovers are triggered by signals received from lower layers. However, the values required for a particular scenario are not specified. Therefore, it is essential to characterize how the use of WLAN signal level thresholds influences the performance of handovers between WLAN and UMTS cells.

Through an extensive simulation study, using a realistic WLAN signal level path loss model and an IEEE 802.21 architecture for the mobile device, we provide insightful guidelines on how the use of signal level information, the chosen criteria to evaluate the signal level and react upon it, and the terminal speed, impacts the handover performance. The results indicate the configuration to be used depends on the value of the primitive *"Link_Configure_thresholds→Link speed"* of the IEEE 802.21 specification. A potential application scenario, could be a IEEE 802.21 based terminal with built-in GPS devices, that could dynamically adjust thresholds' configuration and sampling techniques for WLAN signal level prediction, according with speed variation.

The remainder of this chapter is organized as follows. Section 5.2 introduces the IEEE 802.21 model implemented in the simulator and the handover algorithm developed. Assumptions for both WLAN coverage model and 3G channel emulations are explained in section 5.3. Section 5.4 covers the configuration results, exploring i) the thresholds' configuration, ii) the probability of the packet loss affecting the Mobile IP registration, iii) the different contributions to the losses and iv) the optimal configuration for zero packet loss. Section 5.5 covers the experimental evaluation of the effect of variables in the threshold's evaluation by analyzing, i) the effect of different speeds, ii) the effect of different 3G RTTs and finally iii) the effect of the algorithm selected to measure the signal level. The conclusions are presented in section 5.6.

5.2 Terminal Architecture

In this section we present the model we have used in this chapter. The section contains the following three parts:

- 802.21 Model
- Modification to the Mobile IPv6 stack
- Handover algorithm

5.2.1 802.21 Model

The Media Independent Handover (MIH) functionality has been implemented in the OMNET++[1] simulation tool. It consists of three elements: the MIH Function, the Service

[1] `http://www.omnetpp.org`

Access Points (SAPs) with their correspondent primitives and the MIH Function Services. This is shown in Figure 5.1.

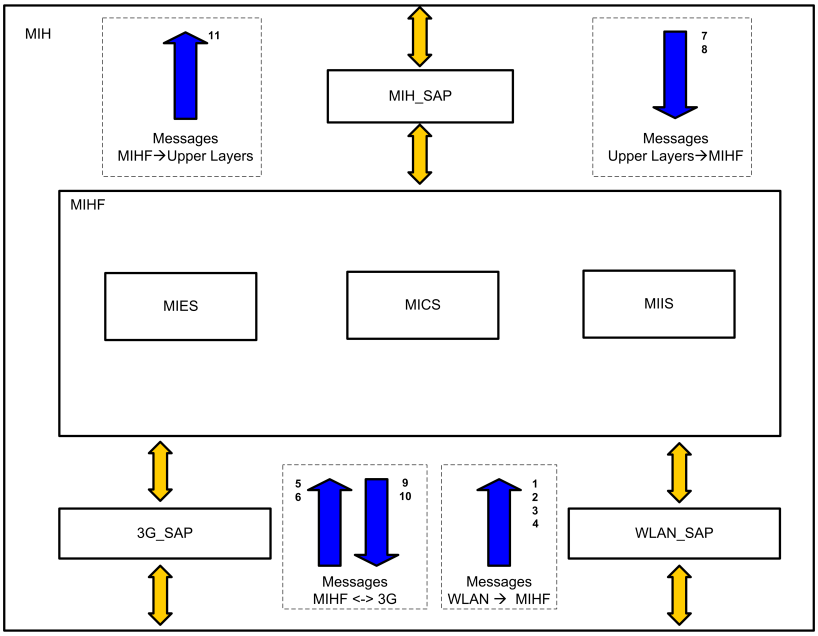


Figure 5.1: IEEE 802.21 MIH OMNET++ model

The MIH Function (MIHF) is defined in the current specification [1] as a logical entity and the specific MIH implementation of the Mobile Node and the network are not included. In fact, it is important to notice that in order to facilitate the overall handover procedure, the MIH Function should be implemented following a cross-layer design, allowing the communication with the management plane of every layer within the protocol stack.

The Service Access Points (SAPs) are used to enable the communication between the MIH Function and other layers. In the presented implementation there is one technology independent MIH_SAP which allows the communication between the MIH function and upper layers, namely IP, transport, and application. Two technology dependent SAPs are also implemented: WLAN_SAP and 3G_SAP, which communicate the MIH Function with the management plane of the 802.11 link layer and the 3GPP link layer, respectively. Note that every SAP defines certain number of primitives that describe the communication with the services in the MIH Function. In this chapter we focus on the MIHO operation of the MN. Since the implemented scenario does not cover all possible use cases, we have defined here only the primitives required by MIHO operation of the MN in the specific scenario studied. Information regarding general primitives of IEEE 802.21 can be found in chapter 2, primitives regarding the coordinated use of IEEE 802.21 and NIHO can be found in the chapter 6.

The MIH Function is supported by three basic services: events (Media Independent Event Service, MIES), commands (Media Independent Command Service, MICS) and information (Media Independent Information Service, MIIS). These services can either

be local or remote. We say that a service is local when the origin and the destination of the service are the same MIH entity, while we say that it is remote when the origin and destination are different entities (e.g., the origin is the mobile terminal and the destination is an Information Server located at the operator network). Since we focus in this chapter on specific scenarios where the terminal does not need to discover neighborhood (Information Services) or to receive remote events/commands from the network, only local communication is taken into account.

The Media Independent Event Service (MIES) (5.1) has been implemented to process some events from the link layers. Currently the model supports the following events:

- Mapping between the MIH_LINK_SAP and the WLAN_SAP:
  - Link_Down: This message is sent by the WLAN_SAP to the MIH Function when no beacon frame has been received within a period of 3 seconds while being connected through the WLAN (Msg 1 in Figure 5.1). This prevents the case of a sudden disconnection from the Access Point (AP) where no disconnection message has been received by the WLAN interface. This event is mapped into the MLME_LinkDown.indication primitive of IEEE 802.11 specification.
  - Link_Up: This message is sent to the MIH Function by the WLAN interface as soon as the WLAN interface receives an association confirmation from the AP (Msg 2 in Figure 5.1). This event is mapped into the MLME_LinkUp.indication primitive of the IEEE 802.11 specification.
  - Link_Going_Down: This message is sent by the WLAN_SAP when the WLAN signal quality is below a certain threshold (Msg 3 in Figure 5.1). This events can trigger an active or passive scan. This event is mapped into the MLME_LinkGoingDown.indication primitive of the IEEE 802.11 specification.
  - Link_Parameters_Report: This message is sent by the WLAN interface to the WLAN_SAP, in order to report the signal strength of the current link. The WLAN_SAP forwards this information to the MIH Function (Msg 4 in Figure 5.1). This event is mapped into the MLME_MREPORT.indication primitive of the IEEE 802.11 specification.
- Mapping between the MIH_LINK_SAP and the 3G_SAP:
  - Link_Up: This message is sent to the MIH Function when the 3G interface is informed that the PDP (Packet Data Protocol) context is started after the activation procedure (Msg 5 in Figure 5.1). At this point data through the 3G interface can be sent. This event is mapped into the SMSM_Activate and the RABMSM_Activate primitives of the 3GPP/3GPP2 specifications.
  - Link_Down: This message is sent to the MIH Function when the 3G interface is informed that the PDP context has been released. (Msg 6 in Figure 5.1). This event is mapped into the SMSM_DEACTIVATE, RABMSM_DEACTIVATE and the RABMAS_RAB_REALEASE primitives of the 3GPP/3GPP2 specifications.
- Communication through the MIH_SAP:

  - MIH_MN_HO_Complete: After a Binding Acknowledgment (BACK) is received by the Mobile IP entity, or after the expiration of the timeout defined to receive a BACK, this message is sent by the MIH_SAP to inform the MIH Function of the handover success or failure (Msg 7 and 8 in Figure 5.1).

The Media Independent Command Service (MICS) provides the means to upper layers to configure, control and obtain information from lower layers. These are the commands defined in our model:

- Commands sent through the MIH_LINK_SAP:
  - MIH_Link_Actions: Through this command the MIHF communicate with the 3G_SAP and the WLAN_SAP to start or finish a connection (Msg 9 and 10 in Figure 5.1).
- Commands through the MIH_SAP:
  - MIH_MN_HO_Commit: This command is sent by the MIH function to inform the Mobile IP entity that a layer 3 handover has to be initiated. The interface towards which the handover has to be executed (i.e., WLAN or 3G) is specified as a parameter of this command (Msg 11 in Figure 5.1).

The goal of the Media Independent Information Service (MIIS) is to create a schema of available neighboring networks with accurate and up to date characteristics values of both upper and lower layers (e.g. Quality of Service QoS on the link, Mobility protocols available in a specific network). Our scenario, as mentioned before, does not require remote communication (the algorithms only use network information available at the terminal).

The MIH Function has always up to date information of the state of both higher and lower layers. Therefore, it will be able to decide when and how a handover procedure should be carried out.

5.2.2 Modification to the Mobile IPv6 stack

In order to have a reasonable control over the handover performance, some modifications to the Mobile IP stack have been implemented.

Mobile IPv6 signaling (Binding Update and Binding Acknowledge) sent by a node for WLAN-3G interworking, could be lost in the network before reaching the destination or could be lost in the wireless medium when the Mobile Node suffers from poor signal conditions. Taking into account that the signaling is always sent through the new link in our implementation, a signaling loss may occur due to varying WLAN signal conditions when moving from a 3G to WLAN. Notice that, as detailed later, we assume in our model no packet loss in the 3G channel. When a BU or BACK is lost the handover at layer 3 is supposed to fail. When the handover fails, the state of the signaling flow can be:

- The BU has not arrived at the Home Agent: the packet flow is reaching the Mobile Node through the old link so no packet loss happens (no handover).

- The BU reaches the Home Agent but the BACK is lost: in this case the packet flow starts arriving to the Mobile Node through the new link. There could be packet loss if the Mobile Node experiences sudden signal condition variation.

Binding Updates are usually retransmitted upon timeout. If a Binding Ack is not received after a timeout expiration, a retransmission is scheduled and the next timeout is set to the double of the original one. This policy is kept until the timeout reaches a maximum (MAX_BINDACK_TIMEOUT is 32 seconds as specified in the Mobile IP RFC [5]).

As the Mobile Node has no way of knowing if the Binding Update has reached the Home Agent or not after a handover failure, the handover algorithm must proceed with an action to stabilize its state. This action is to perform a handover to the 3G leg.
The major modification introduced into the Mobile IP stack is in the way the retransmission of the Binding Updates is handled. The retransmission algorithm of Mobile IPv6 introduces strong delays if any of the packets implied (Binding Update and Binding ACK) are lost. Even more important, once the MIPv6 registration starts, in the current implementation, it cannot be stopped, being retransmitted the Binding Updates until an Binding Ack is received or a maximum timeout (in the order of tens of seconds) is reached. If a good user experience wants to be provided, in the case of a terminal with multiple technologies there are scenarios where it is worth to stop the current MIPv6 registration which is experiencing a high delay due to registration messages being lost and perform a handover to other available technology.
In our model we decided to take out the retransmission part of MIPv6 and handle the needed retransmissions in the algorithm controlling the handover. When a Binding Update is sent, triggered by the MICS module, the Mobile IP module sets a timeout of 1.5 seconds (timeout of the first BU transmission as specified in [5]). After this timeout expires, a message indicating the failure of the handover is sent to the MIH layer, which takes the required actions (namely rolling back to the 3G channel).

5.2.3 Handover Algorithm

In order to handle the complexity of the scenario a control algorithm has been implemented. This algorithm is defined as a MIH User which should be implemented as an entity out of the MIHF, interfacing with it by the MIH_SAP. Our handover algorithm is based on signal thresholds. It relies on the information provided by the Media Dependent layers and the Mobile IP Layer. A complete flow diagram of the handover algorithm is presented in Figure 5.2.

The handover algorithm reacts upon the reception of three possible signals, which are:

- RSSI (Received Signal Strength Indicator) sample
- Notification about the status of the handover
- Wireless LAN link off message

The handover algorithm is based on two thresholds. The first one, $3G \rightarrow WLAN$ threshold, defines the minimum wireless LAN signal level that must be received in the

Mobile Node to trigger a handover from the 3G to the wireless LAN. The second one, $WLAN \rightarrow 3G$ threshold, defines the wireless LAN signal level below which a handover to the 3G leg is triggered.

A handover to the wireless LAN is performed when the signal level reaches the value specified by the $3G \rightarrow WLAN$ threshold. The mean value of the two last samples of signal level is taken in order to measure the signal level; with this the signal level variability is decreased. A handover to 3G is performed when the signal level goes below the $WLAN \rightarrow 3G$ threshold, or when a WLAN Link_Down event is received.
The philosophy of the algorithm is to try to maximize WLAN use when possible and keep connections through 3G otherwise.

After the MICS triggers a handover to the Mobile IP Layer, the handover algorithm is not allowed to perform another handover until the reception of a handover status message informing of the last handover result. If a handover is not successful, the algorithm performs a handover to the 3G part to fix the state of the algorithm. There are different causes for the failure of a handover. The BU may not reach the Home Agent or the BU reaches the Home Agent but the Binding Ack is lost.

Before performing a handover some conditions must be satisfied. The interface should be completely configured, with a global routable IPv6 address (Duplicate Address Detection (DAD) procedure completed) and default router associated. Also, all previous handovers should have been completed. If these conditions are not fulfilled the handover is delayed. In the case of handover to WLAN, if the conditions are not met, the handover is skipped until another signal sample arrives. In the case of handover to 3G, the handover is delayed by a timer, waiting for the conditions to be satisfied. The timer has been fixed to 100 ms. The value of 100 ms is the default period of the beaconing in WLAN. The retrial of a handover to the 3G is performed each time the signal level goes down the $WLAN \rightarrow 3G$ threshold. If any of these trials is successful before this timer expires, the timer is cancelled. The main purpose of this timer is to assure the retrial even if the MN is out of the wireless LAN cell, in this case the Mobile Node will not receive a frame in the 100 ms period and the timer will retry the handover even if no power indication arrives.

5.3 Simulation Setup

The handover study has been conducted by simulating a mobile node attached to the 3G network and performing several handovers between 3G and wireless LAN.

The specific scenario analyzed is based on an indoor environment with several non-overlapping wireless LAN cells and a full coverage of 3G technology. We argue that this represents a scenario that will be a typical deployment in the future. Please note that this work does not cover the WLAN to WLAN handover case. This work considers a wide space with indoor characteristics in which the user could move faster than walking speed, such as in an airport using, for example, an electric vehicle.

The Mobile Node speed is fixed to 10 m/s for the first part of this chapter where the effect

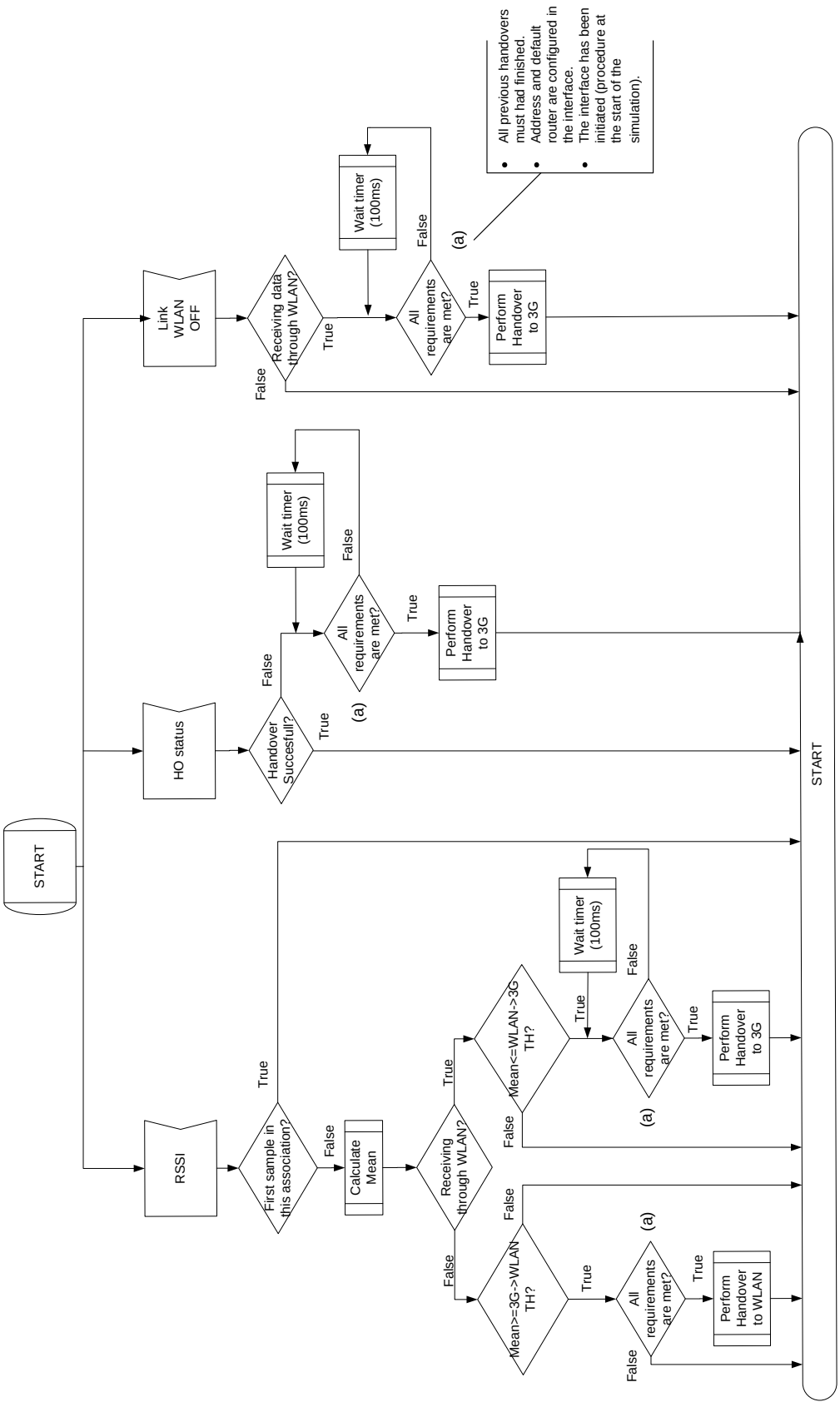


Figure 5.2: Handover Algorithm Flow Diagram

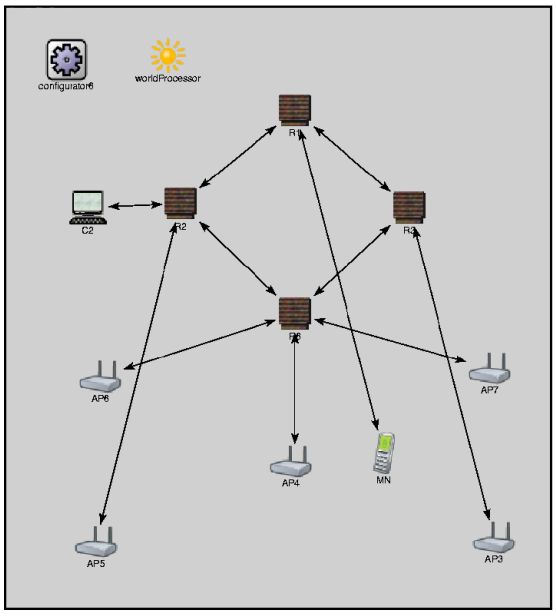


Figure 5.3: Simulated Scenario

of the threshold configuration wants to be analyzed. For the second part of this chapter, where the effect of the speed on the threshold configuration is studied, the speed is varied between 2 m/s and 10 m/s. This value represents an upper limit of the speed expected in the big size indoor scenario. Indeed, all pedestrian speeds are well below this threshold.
The movement pattern selected is the Random Way-Point Model. With this model each node moves along a zigzag line from one waypoint to the next one, all the waypoints being uniformly distributed over the movement area.
The traffic studied is a downstream audio, with a packet size of 160 bytes at application layer and inter-arrival packet time of 20 ms (83 kbps). Notice that usual VoIP codecs generate bit rates around 80 kbps. 60 simulation runs were performed for each experiment. This number was chosen as a tradeoff between simulation time and confidence interval. In Figure 5.3 a schematic view of the simulation scenario is shown. The audio server is the node C2, the Home Agent is the Router R1 and the Mobile Node is the phone MN. The line connecting MN and R1 is the emulated 3G channel. The Round Trip Time between the node C2 and the Mobile Node has been taken equal to 350ms for the 3G leg of the MN and equal to 150ms for the Wireless LAN. The RTT of 150ms using the WLAN leg is higher than most real scenarios, and is chosen to test our algorithm in a worst case situation.

5.3.1 WLAN Model

The standard wireless LAN propagation model defined in OMNET++ is based on free space losses with shadowing and a variable exponential coefficient. The original model implemented in OMNET++ is suitable for studies that do not analyze in depth the effect of the signal variation. However, the objective of this work is to have a realistic wireless LAN model, suitable for indoor scenarios based on empirical results. For this purpose, we

used the empirical model in [84] [85] and [86], which includes variation in the signal due to shadowing and different absorption rates in the materials of the building. The path loss model is the following:

$$\begin{aligned} Losses &= 47.3 + 29.4 * log(d) + 2.4 * Y_s \\ &+ 6.1 * X_a * log(d) + 1.3 * Y_s * X_s \\ X_a &= normal(0, 1) \\ Y_s &= normal(-1, 1) \\ X_s &= normal(-1.5, 1.5) \end{aligned} \tag{5.1}$$

being *d* the distance between the Access Point and the Mobile Node.

The power transmitted by the AP and Mobile Node are defined in the UMA specification [87], [88]. The AP transmission power is 15dBm while the Mobile Node transmission power is 10 dBm. Following these specifications, the AP antenna gain is set to 0 dBi while the Mobile Node antenna gain is set to -10dBi. The transmission rate of the wireless LAN is fixed to 11 Mbps.

Taking into account these values and the equation for the looses (equation 5.1), the maximum and minimum cell radius for both stations can be calculated:

- AP maximum cell radius: 283.38 m
- AP minimum cell radius: 60.88 m
- Mobile Node maximum cell radius: 39.99 m
- Mobile Node minimum cell radius: 12.03 m

The minimum and maximum cell radius for the MN and AP are calculated by clearing from the equation 5.1 the distance and calculating it for the different transmission powers and the maximum and minimum signal attenuation given by the model, against the sensitivity.

The OMNET++ wireless model defines two thresholds, the Sensitivity threshold and the Active Scanning threshold. The Sensitivity threshold is the minimum level of signal that the receiver can detect. Real products specifications set this level of signal to -90 dBm[2]. This is the value that we have used in our simulations. The Active Scanning threshold defines when the wireless card starts scanning for other APs in order to perform a WLAN to WLAN handover. When this level of signal is reached the Mobile Node detaches from the current AP. The IEEE 802.11b specification does not specify the value for this threshold, its value being design dependant. In the model presented, this value is set to -80 dBm. This value was selected after analyzing via simulations the maximum variability of the wireless LAN signal model. With this threshold we gain that the Mobile Node disconnects from the AP before reaching the sensitivity threshold.

[2]SMC Networks SMC2532W-B

5.3.2 3G channel Model

The 3G channel has been modeled as a Point to Point Protocol (PPP) channel with a connection time of 3.5 seconds, disconnection time of 100 ms, bandwidth of 384 kbps (downlink) and a delay of 150 ms per way (300 ms Round Trip Time (RTT)). The above PPP channel models the 3G channel when the Protocol Data Packet (PDP) context is activated. The disconnection and connection times were measured in different locations of an office building with a commercial UMTS data card. The round trip time is tuned to a typical value of delay in this kind of channel under the same conditions. The connection time is measured as the time elapsed between bringing up the card and the moment when an IP address is assigned to the Mobile Node (activation of a PDP context). Although the model takes into account the connection time, we have assumed that the PDP context is always active, so the value of the connection time does not have any impact on the simulations.

Our simulations are based on i) full 3G coverage and ii) 3G link always on, which we argue that are realistic assumptions in typical scenarios.

5.4 Analysis of the threshold configuration on the handover performance

The results obtained can be classified in three different categories. First, an analysis of the *Wireless LAN utilization time versus the number of handovers* is presented, as a metric of the performance of the algorithm. Second, an analysis of the *probability of losing a Binding Update is performed*, to understand the effect of the algorithm on the control plane.
The packet loss due to *signal variation* and its behavior as a function of the threshold are analyzed to detect the impact of the different thresholds in a realistic environment modeled by the wireless signal model used. Finally, the *percentage of the different contributions to the packet loss* is studied to find the right tradeoff between seamlessness requirements and packet loss. The study is complemented with an *analysis of the performance of the algorithm in the configuration for zero packet loss*. The simulations have been divided in two stages. First, we evaluated a wide interval for both thresholds (i.e. $3G \rightarrow WLAN$ in the interval [-80, -65] dB and $WLAN \rightarrow 3G$ in the interval [-80, -70]) to understand the trend of the algorithm's behavior. In a second stage we selected relevant points to find the threshold values that achieve zero packet loss, this metric being the final goal of simulation study.

5.4.1 Wireless LAN utilization time

Figure 5.4 shows the time the wireless LAN is used per handover and the number of handovers performed for several combinations of both thresholds.
It can be seen that as the threshold $3G \rightarrow WLAN$ (in dBm) increases, the number of handovers decreases, but the time a station stays in the WLAN increases. This shows that, by setting the $3G \rightarrow WLAN$ thresholds to a value large enough the algorithm can be configured to avoid useless handover. In this way, only handovers that allow the Mobile Node to be connected for a longer time to the WLAN APs are performed while excluding short stays. This feature is desirable and ensures that only handovers increasing user WLAN experience are performed.

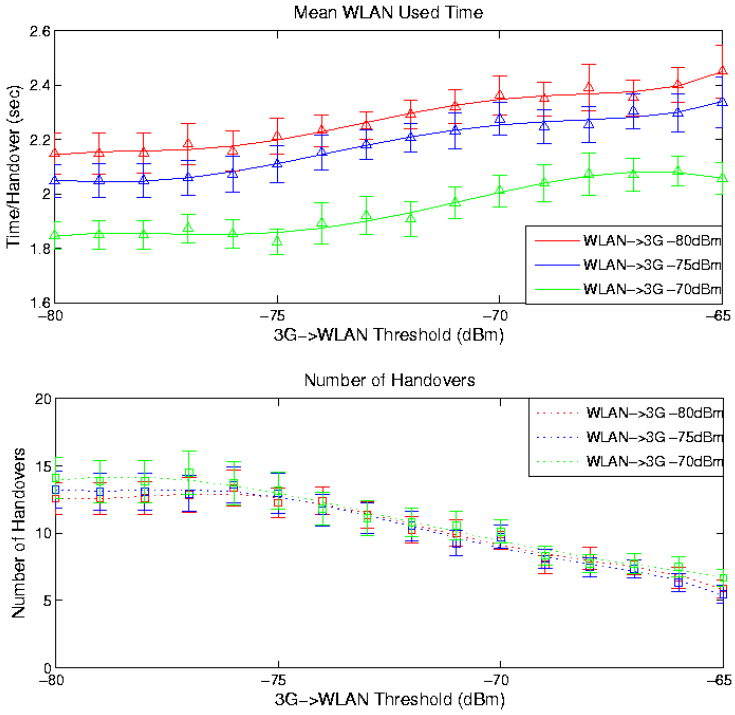


Figure 5.4: Wireless LAN Time usage and number of handovers

Although the number of handovers only depends on the $3G \rightarrow WLAN$ threshold, the wireless LAN utilization depends on the $WLAN \rightarrow 3G$ threshold too. As expected, in the figure we can observe that the wireless LAN utilization time increases as the $3G \rightarrow WLAN$ threshold increases (in dBm). This growing trend is maintained while increasing (in dBm) the $WLAN \rightarrow 3G$ threshold.

5.4.2 Binding Update loss probability

The main reason for BU losses is caused by the fact that the MN tries to perform a handover to wireless LAN when the signal level is not good enough. In this situation the BU or BACK can be lost. The data losses associated to this event occurred because the Home Agent cannot send data through the wireless LAN link, when the MN is not present on the cell or even when it is present but the signal level is poor.

Figure 5.5 plots the probability of losing a Binding Update for varying thresholds. For all the configurations simulated there is one threshold that allows all handovers to be performed without losing any Binding Update. For completeness all the possible configurations of the thresholds have been simulated. In Figure 5.5 (and all successive) it must be noted that the number of packets lost is always minimized under the condition $3G \rightarrow WLAN(dBm) > WLAN \rightarrow 3G(dBm)$. This is because when $3G \rightarrow WLAN(dBm) <= WLAN \rightarrow 3G(dBm)$ there is a ping pong effect in the 3G to WLAN handover, the mobile device executes a handover from 3G to WLAN because the

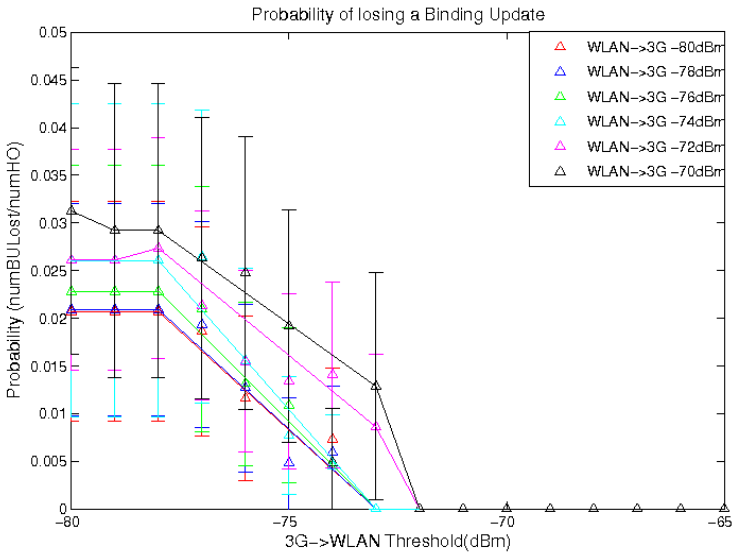


Figure 5.5: Probability of losing a Binding Update for several thresholds

WLAN signal level is greater than the $3G \rightarrow WLAN$ threshold, but immediately handovers back to 3G because the WLAN signal level is below the $WLAN \rightarrow 3G$ threshold.

The Binding Update losses depend heavily on the $3G \rightarrow WLAN$ threshold. It can be seen in Figure 5.5 that there is a level of this threshold (-74 dBm) in which Binding Update losses are reduced to zero. In the figure we can see also a dependency of Binding Update losses with the $WLAN \rightarrow 3G$ threshold, this is only because the ping pong effects explained before if $3G \rightarrow WLAN(dBm) <= WLAN \rightarrow 3G(dBm)$.

5.4.3 Losses due to signal variation

The losses due to signal variation appear as an effect of the oscillation in the signal level. Even when the wireless signal level is not sufficiently weak to trigger a handover to the 3G leg, fading or a high negative variation of the signal produces a loss of several packets. These losses depend on the distance to the Access Point. Fading can happen by a third moving object (e.g. a person walking near the AP) or by the movement of the MN (i.e., when going through a metal door or wall).

Figure 5.6 shows several histograms for the packet loss due to variation of the signal. The X axis represents the number of packets lost (each time a loss due to signal variation occurs). The Y axis represents the probability of this packet loss. As the threshold $3G \rightarrow WLAN$ (in dBm) is increased for a fixed $WLAN \rightarrow 3G$ threshold the losses due to signal variation vary from the positive values to zero. This behavior is the expected one since the signal variation depends on the distance between the Mobile Node and the AP. If the $3G \rightarrow WLAN$ threshold increases, these losses decrease. In Figure 5.6, the right hand histogram shows how the probability of zero packet loss increases when the $3G \rightarrow WLAN$ threshold is configured to trigger handovers only when the terminal is close to the AP.

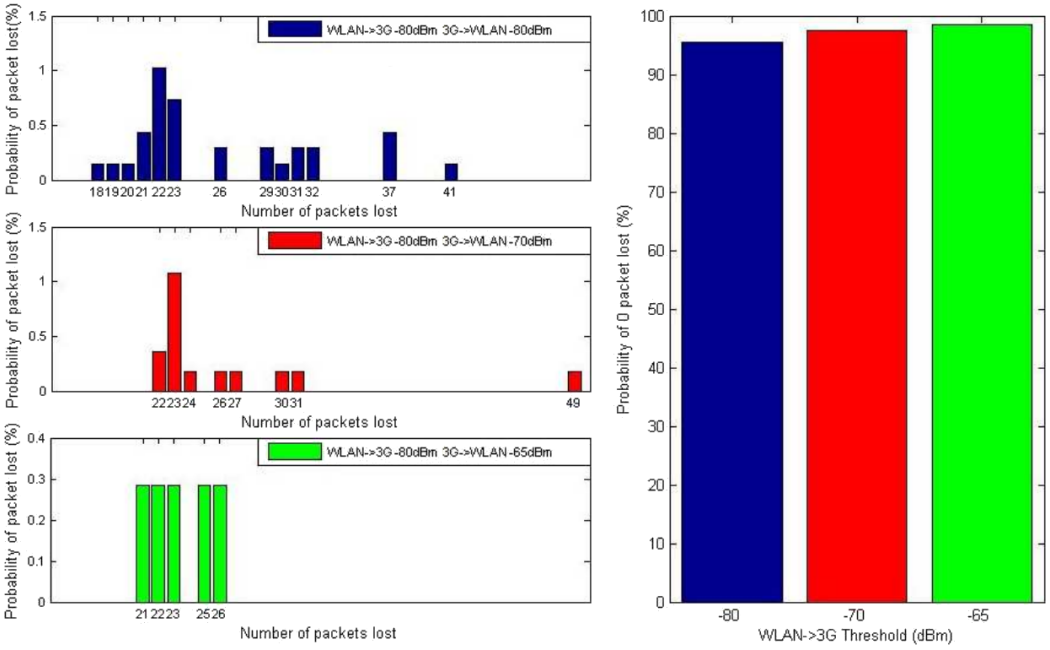


Figure 5.6: Effect of the thresholds in the packet loss due to variation of the signal level

5.4.4 Study of the different contributions to packet loss

Figure 5.7 shows a study of the different contributions to the global packet loss for three different thresholds. The major reason for packet loss in all the configurations is the handover to the 3G leg. Losses due to signal variation, that start just before a handover to 3G and finish after the Home Agent has received the Binding Update (and the packets are sent through the 3G channel), are accounted. The contribution to the packet loss because a Binding Update procedure fails, is less relevant. It tends to disappear after the $3G \rightarrow WLAN$ threshold of -74 dBm is crossed. The loss due to signal variation appears for all thresholds but its effect decreases when the $3G \rightarrow WLAN$ threshold increases (in dBm). The losses in the case of handover to the 3G channel are mostly affected by the $WLAN \rightarrow 3G$ threshold, as can be seen in the bottom graph of Figure 5.7.

In all the studies performed the minimum packet loss is of 14 packets/handover, a quantity that can be supported by an appropriate buffer in the application layer in most scenarios, although it can be a problem for applications with delay requirements. In next sub-section we explore the needed thresholds to achieve zero packet loss.

Note that the time required by the mobility signaling does not have an impact on the packet loss, since the MN keeps using the old interface until the handover is completed. Hence, there is no interruption on the packet flow while the handover is ongoing.

5.4.5 Zero Packet Loss

Figure 5.8 shows the wireless LAN utilization time, the number of handovers performed and the packet loss trend when a the threshold configuration for zero packet loss is

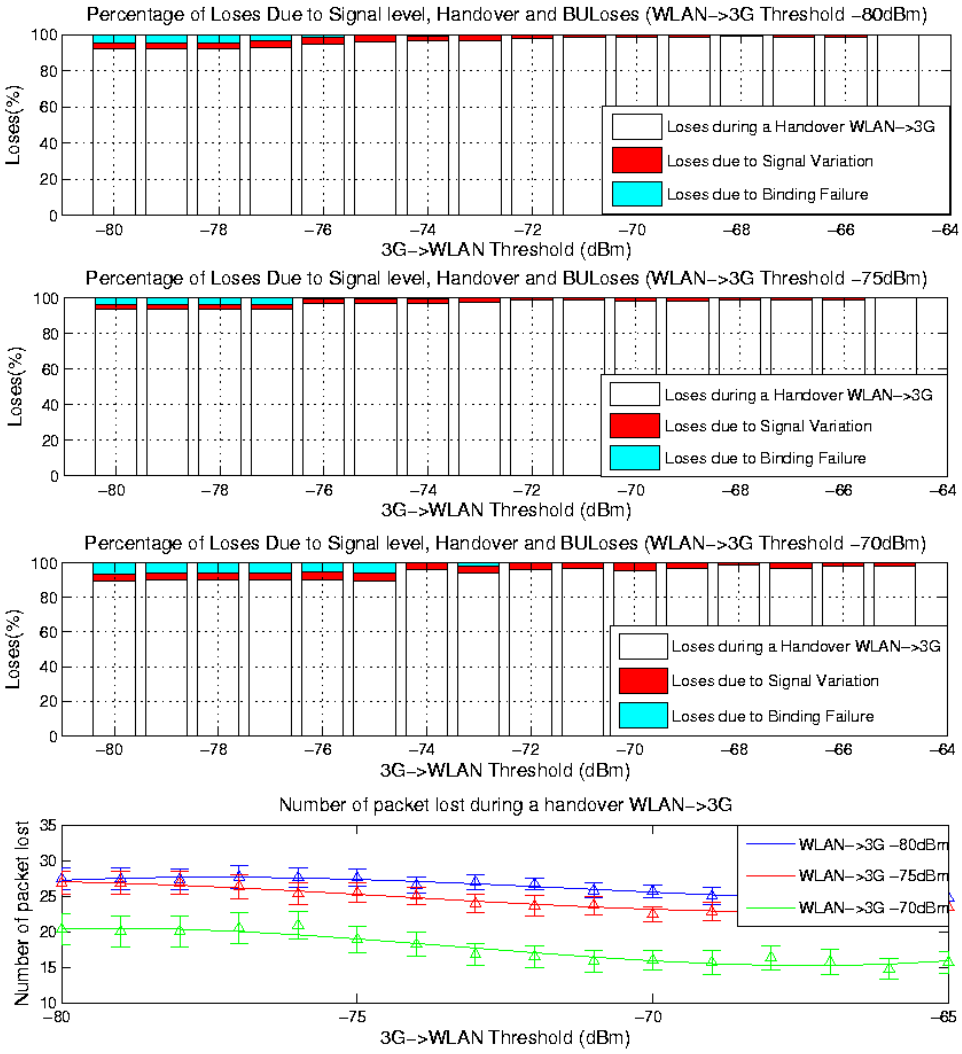


Figure 5.7: Study of the different contributions to the packet loss

considered. Zero packet loss can be achieved when a high $3G \rightarrow WLAN$ (in dBm) (namely $3G \rightarrow WLAN$ value is -55 dBm) threshold is used, to eliminate the losses due to Binding Update losses and signal variation. Also a high $WLAN \rightarrow 3G$ (in dBm) threshold is needed to reduce packet losses due to signal variation, although this threshold must be lower than the $3G \rightarrow WLAN$ threshold to avoid ping-pong effects. In the results obtained, with the values $3G \rightarrow WLAN = -55dBm$ and $WLAN \rightarrow 3G = -66dBm$, we achieve seamless handovers.

The penalty imposed for the use of such high thresholds is clear since the number of handovers is drastically reduced. Note that the plots shown correspond to samples where handovers had taken place. A 30% of the samples obtained, did not contain any handover, in contrast with the other configurations showed previously where all samples presented

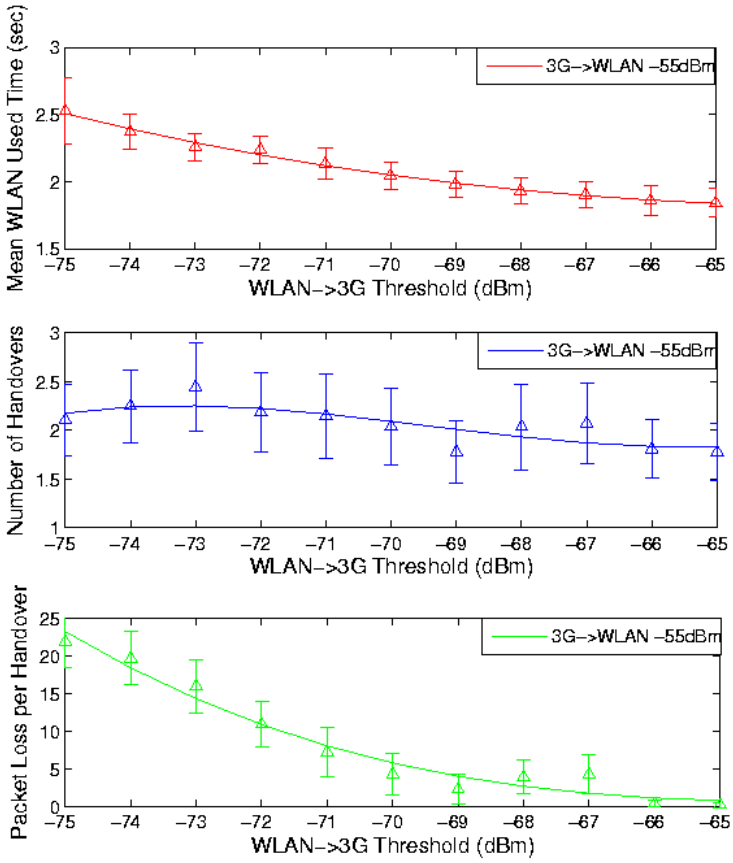


Figure 5.8: Study of the performance obtained for 0 packet loss

handovers. The plots therefore represents relative values to such conditions.

The Mean Wireless Utilization Time, shown in Figure 5.8, depicts a decreasing slope while the $WLAN \rightarrow 3G$ increases (in dBm). This behavior was noticed previously. The Wireless Utilization Time for a given $3G \rightarrow WLAN$ (in dBm) threshold decreases while increasing the $WLAN \rightarrow 3G$ (in dBm) threshold.

The number of handovers presents a stable shape, as the difference between the thresholds is greater than the signal variation, no ping pong effect occurs. The absolute number of handovers is small (approximately 2 handovers) and depends on the $3G \rightarrow WLAN$ threshold. If this threshold is high (in dBm), the Mobile Node must be very near the AP to perform a handover.

The packet loss per handover decreases dramatically until the $WLAN \rightarrow 3G$ threshold reaches -70 dBm. It then tends to zero for $WLAN \rightarrow 3G = -66dBm$.

5.5 Analysis of the effect of mobile terminal speed on the handover performance

In this section we present the handover performance study considering the following metrics:

- Wireless Utilization Time
- Number of Handovers
- Packet loss

In a first step, an analysis of the three metrics for different configurations of the thresholds is performed. Speed varies between 2m/s and 10m/s (Section 5.5.1). In a second step the study is extended by introducing the RTT in the 3G channel as additional variable (Section 5.5.2). The way which WLAN signal level is evaluated impacts the overall handover performance, for this reason, we have considered (and compared) several measurement techniques (Section 5.5.3).

5.5.1 Effect of the speed in the thresholds configuration

Figures 5.9 to 5.11 show how the algorithm behavior changes depending on the speed.

Figures 5.9 and 5.10 respectively show the amount of time the Mobile Node is connected to the WLAN and the number of handovers performed by the Mobile Node. It can be observed that while the number of handovers decreases when more stringent thresholds are configured, the Wireless utilization time increases. This shows that the proposed algorithm (based on two thresholds), if properly configured, can optimize the wireless utilization time by reducing the number of useless handovers. Another interesting observation is that as the speed decreases, the difference in the wireless utilization time for different speed values increases.

Figure 5.11 shows the number of packet losses during the handover. All the curves of figure 5.11 show a common behavior. Note that losses can be either due to signal variation or due to handover failure. As the $WLAN \rightarrow 3G$ threshold increases, losses (both due to signal variation and to a handover failure) are reduced. We define the threshold configuration for zero packet loss, as the configuration of both thresholds in the Mobile Node with which a seamless handover is possible. The threshold configuration for zero packet loss varies for the different speeds. For speed value of 2m/s a configuration of $WLAN \rightarrow 3G = -70dBm$ and $3G \rightarrow WLAN = -70dBm$ is enough to provide zero packet lost. However, for the same threshold configuration and speed about 10m/s, on average 20 packets are lost. These values give insightful information for optimal terminal configuration and handover performance.

5.5.2 Effect of the 3G channel RTT in the threshold configuration

To complete the study, an analysis on how the RTT of the 3G link affects the thresholds' configuration is provided. Figure 5.12 shows how the 3G channel RTT affects the Wireless

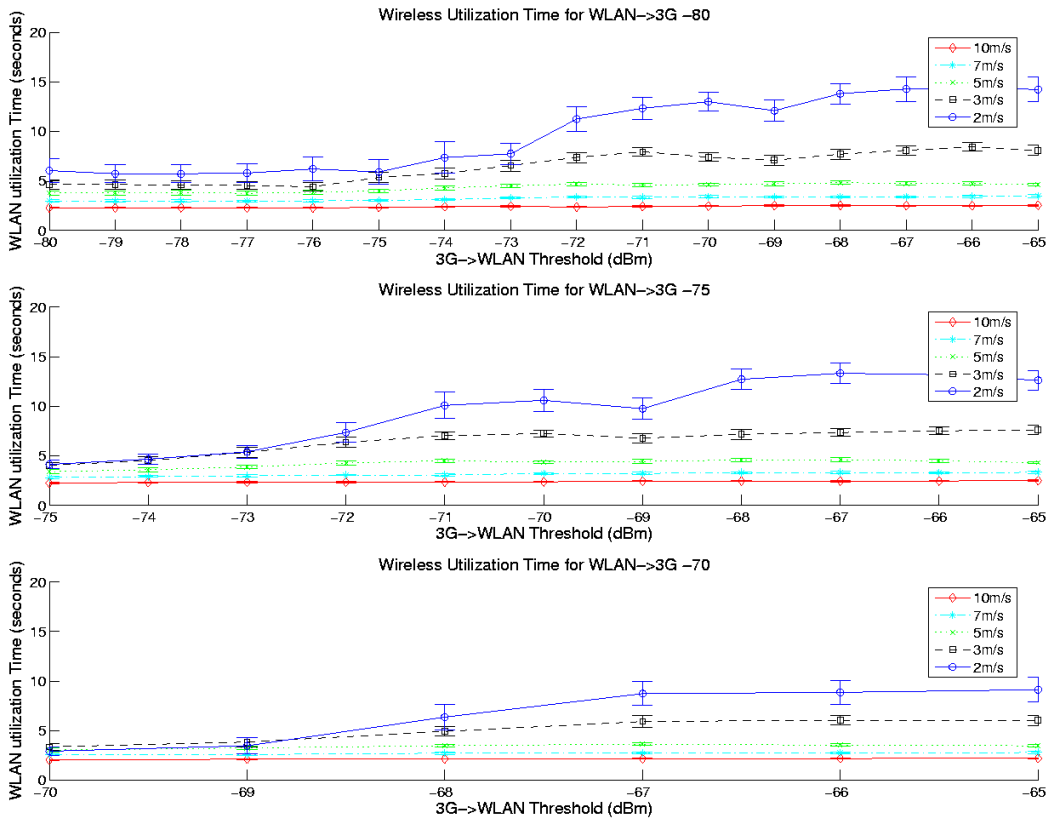


Figure 5.9: Wireless Utilization Time for several speeds (RTT 3G 300ms)

utilization time, the number of handovers and the packet loss for a specific threshold configuration. Following typical values of RTT for an UMTS channel, which range between 190ms and 220ms[3], we vary RTT between 200ms and 300ms (i.e. the values used in the study are a worse case estimation). Figure 5.12 shows that RTT affects neither the wireless utilization time nor the number of handovers performed. The major effect is in the number of packets lost. The reason is as follows. Since the RTT increases the time required to handoff to the 3G leg, the number of packets lost (due to WLAN signal level fading) increases accordingly. The effect is the same as if a less restrictive value for the $WLAN \rightarrow 3G$ threshold is used.

5.5.3 Effect of the speed in the algorithm for measuring the signal level

As our handover algorithm is based on signal power thresholds and the signal level can typically vary a lot in different environments, the information reaching the MIH layer (e.g. RSSI each beacon interval) can be different in a relative short amount of time. Therefore, taking into account last samples, or a series of samples is not sufficient to derive the trend of the signal conditions. Thus, we propose several approaches to infer the real trend of

[3]Values measured with a commercial data card.

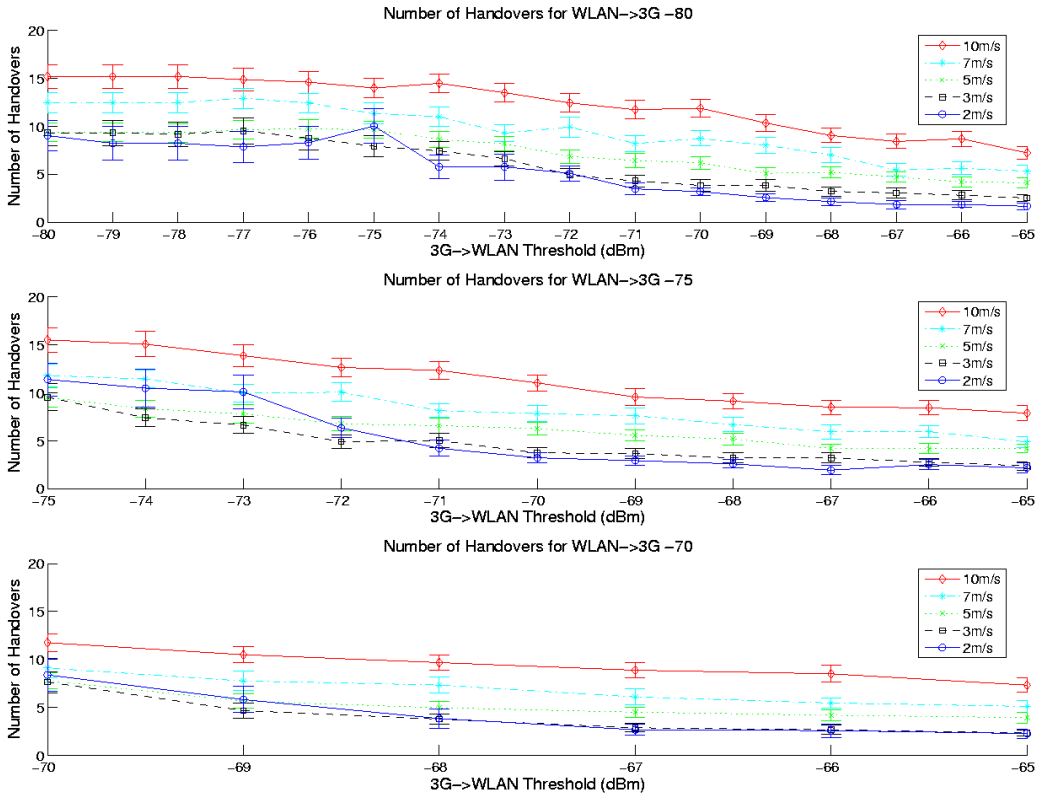


Figure 5.10: Number of Handovers for several speeds (RTT 3G 300ms)

the signal (based on beaconing interval) against different speed conditions. The different algorithms analyzed are:

- Single Sample (SS): The current value of the signal is the last beacon. $y[n] = x[n]$
- Weighted mean (WM): The current value of the signal is the value given by a weighted mean between the last beacon and the previous one. $y[n] = \alpha x[n-1] + \beta x[n]$
- Weighted mean with the previous mean (WMPM): The current value of the signal is the value given by the weighted mean between the last sample and the last mean. $y[n] = \alpha y[n-1] + \beta x[n]$
- Weighted mean of three samples (WM3S): The current value of the signal is the weighted mean between the last three samples. $y[n] = \alpha x[n-2] + \beta x[n-1] + \gamma x[n]$

Taking into account the four proposed algorithms, a simulation in Matlab has been performed. For each algorithm, the optimal parameters of the weighted mean have been computed (trying all the combinations) taking into account several speeds. Figure 5.13 shows the Mean Error square obtained while evaluating the signal level for [SS], [WM],[WMPM] and [WM3S] techniques. From the results, it can be seen that for low speeds the algorithm *Weighted mean with the previous mean (WMPM)* outperforms the others, while for high

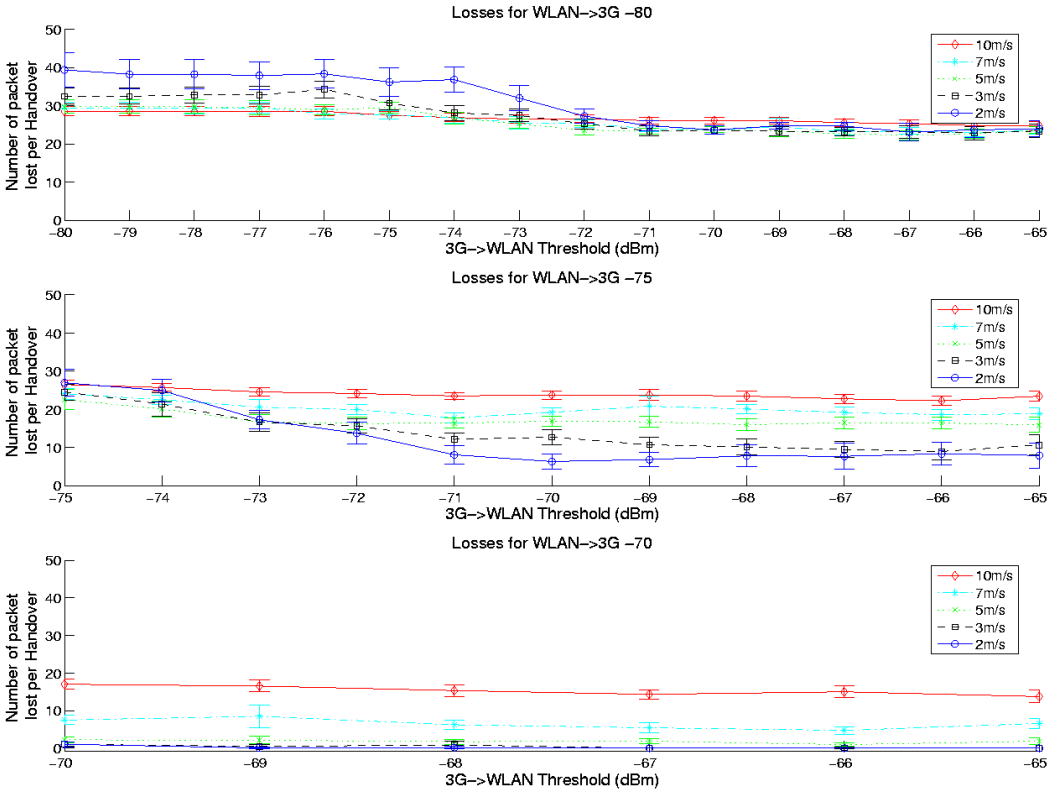


Figure 5.11: Number of Packets Lost for several speeds (RTT 3G 300ms)

speed the algorithm *Weighted mean of three samples (WM3S)* gives the best performance. Based on these results, we recommend a combined approach dependent on terminal speed. Table I presents the optimal configuration for the two recommended algorithms.
As an additional example, we could consider the case of a terminal moving at 2 m/s. The optimal sampling technique is the WMPM and the optimal threshold configuration values are -75 dBm for $WLAN \rightarrow 3G$ and -70 dBm for $3G \rightarrow WLAN$. These values (not affected by the RTT) optimize Wireless LAN utilization time while providing acceptable packet loss rate. In a similar way, results can be derived from the graphs for other speeds and RTT.

5.6 Conclusions

In this chapter we have presented a terminal architecture which tightly integrates the IEEE 802.21 specification with Mobile IPv6. This framework is completed with an intelligence which is able to detect the communication requirements of the user and adapt the technologies being used to maximize the user experience. The integration of such technologies presents several challenges which have been described and studied along this chapter. The IEEE 802.21 standard defines an architecture for terminals to support handovers between heterogeneous networks in a technology independent way but it does not

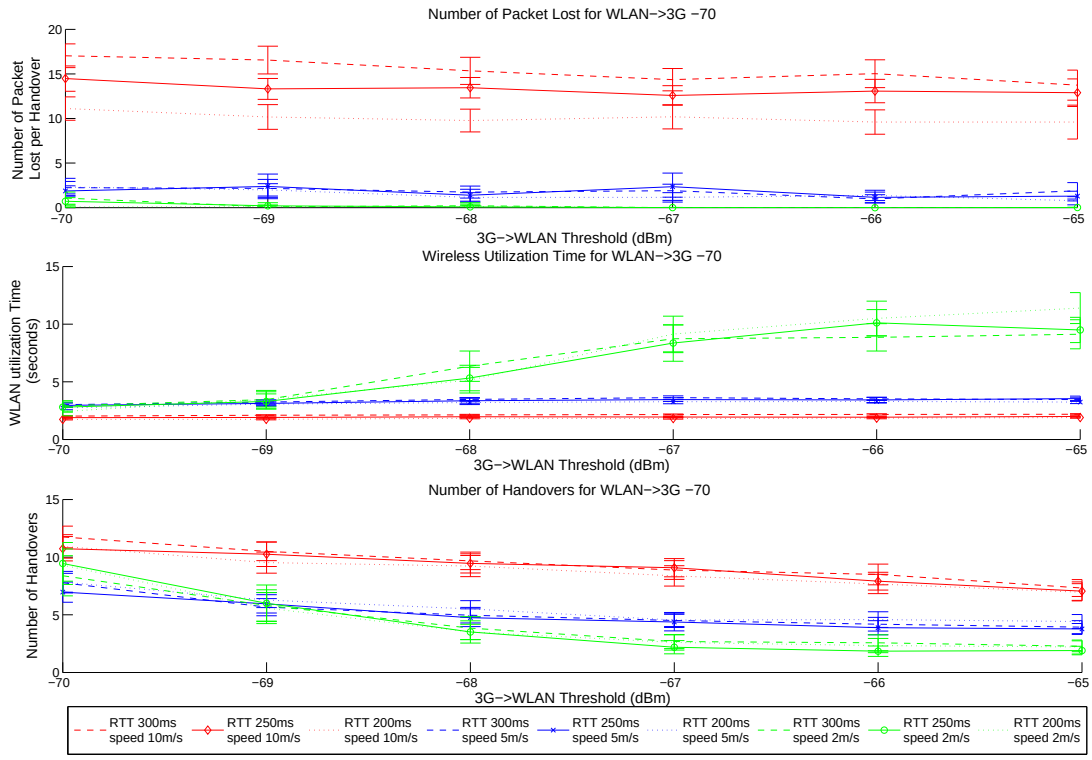


Figure 5.12: Wireless Utilization Time, Number of Handovers and Number of Packets Lost for several speeds and RTTs in the 3G Link

define how the handover decisions should be made. Basically the standard defines the tools that can be used but it does not define which must be used or how they should be used. In this framework we analyze architectural issues and integrate, in a simulation environment, layer two and layer three functionalities. Within this framework an algorithm is evaluated taking into account several metrics such as WLAN utilization time while minimizing the number of handovers and packet loss.

The work presented in this chapter studies, by means of simulation (using OMNET++), a typical scenario with UMTS universal coverage and islands of WLAN coverage. If WLAN coverage is available, it is preferred because of cost and bandwidth reasons. We have defined an architecture for the mobile terminal based on the IEEE 802.21 work and the use of Mobile IPv6 to manage IP mobility. Handover decisions are taken by means of two WLAN signal level thresholds, one to decide a handover from 3G to WLAN, and a different one to decide when to handover from WLAN to 3G. The algorithm for handover decision has two objectives: maximize WLAN utilization and minimize service discontinuity. In this chapter we have explored the influence of the thresholds for handover decision on these parameters, namely, WLAN utilization and packet loss, taking into account the interaction

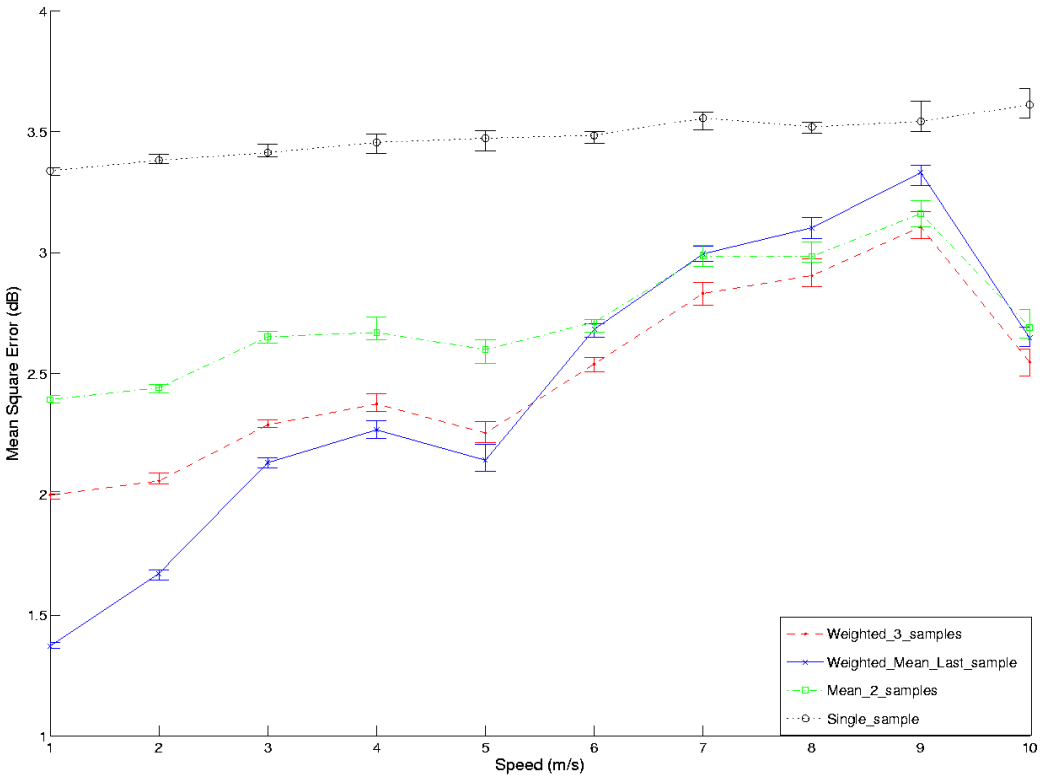


Figure 5.13: Mean Square Error of the signal behavior prediction for different sampling algorithms

with Mobile IPv6 behavior.

The results obtained allow us to observe the trade-off between service continuity and WLAN utilization. The two defined thresholds proved flexible enough to manage this trade-off, allowing configurations with packet loss and high WLAN utilization, and also configurations with zero packet loss although achieving a much lower WLAN utilization. In this way, we showed that, by configuring the two thresholds, we can adapt the mobile terminal behavior, with respect to handover decisions and to user preferences. Another interesting result of the work has been to see the flexibility that the IEEE 802.21 architecture showed for implementing policies for handover decisions managing the interaction with upper and lower layers.

The mobile terminal speed used in the simulation study (2-10 m/s) can be considered a worst case for the studied scenario (pedestrian speed or slow moving vehicles are below that speed). The results obtained show the impact of terminal speed and the RTT between the operator (Home Agent) and the Mobile Node, on the handover performance. Based on these results guidelines for thresholds configuration to achieve zero packet loss have been provided. This is in line with current IEEE 802.21 specifications. Indeed, the

Speed	WMPM		WM3S		
	α	β	α	β	γ
1m/s	0.2	0.8			
2-3m/s	0.3	0.7			
4-5m/s	0.4	0.6			
6m/s			0.4	0.4	0.2
7-9m/s			0.5	0.3	0.2
10m/s			0.6	0.3	0.1

Table 5.1: Optimal parameters for the configuration of the *WMPM* and *WM3S* algorithms

standard defines protocol operations to configure thresholds for triggers to be generated, while in this work we have complemented the standard by finding the optimal thresholds for this configuration. In a environment with variable terminal speeds, signal strength measurements need to adapt to this dynamic environment by using sampling techniques to filter out spurious variations. To this aim, we have found that a combined approach, modifying the sampling algorithm depending on the speed, is the more suitable.

Finally, it is worth to note that the performance experienced by the user can be improved by a coordinated operation of the Mobile Node and the network. The IEEE 802.21 provides capabilities for obtaining and using information or commands originated by the network which integrated in future algorithms enables the use of a full view of the network in handovers decisions. This view cannot be obtained by the Mobile Node by its own means and its use can boost the performance of the network, under the user's and operator's viewpoint. We explore the possibilities of this kind of solutions in the next chapter (see chapter 6).

Part IV

Network Controlled Handovers

Chapter 6

Integrating Network Controlled Mobility on 4G Networks

6.1 Introduction

In previous chapters we have presented the way of integrating the upcoming IEEE 802.21 specification and Mobile IPv6 in a terminal, providing configuration recommendations to achieve the goal of seamless handovers. As presented in chapter 4 a way of improving the performance experienced by the end user and the resource utilization of the network is a coordinated operation of network and terminal with a common goal: achieve seamless handovers providing the user with the required quality of service, all of this while maximizing the network utilization.

Traditional Mobile Initiated Handovers (MIHO) are triggered by mobile devices upon collection of events such as radio signal level degradation, application requirements or the like. MIHO mechanisms can be further improved by retrieving from the access network information [89] about available bandwidth, network load in a specific access point/access router, etc. It would be desirable to gather information in the access network about load conditions (in a network-to-network relation) as well as from mobile devices (in a mobile to network relation) leading to the composition of an accurate and dynamic map that handover decision engines could benefit of. However, we argue that disclosing such information to mobile devices is subject to access network policies and might not always be possible to provide such data, and even with that information a terminal cannot have a global view of network requirements. On the other hand, in such complex environments the network should be able to decide on how its resources are distributed, even in a MIHO scenario. For example the network may reject a handover if the target access point is overloaded. The mobility paradigm in which the network has the final decision about the handover of a terminal is called Network Controlled Handover (NCHO), following the definition given in [55], and is the subject of this chapter. Scenarios where the network has the final decision about the handover are suitable for optimizations, in such a case, the network can also decide to move some users to other access point or even access technology to optimize the network resources or utilization. This concept, in which the network decides and initiates a handover, is called Network Initiated Handover (NIHO). Hence, NIHO via a centralized

approach aims at improving network operations where required. The concept of MIHO and NIHO applies to both intra technology case or inter technology case, the former being potentially layer two specific, the latter leading to an IP based approach.

A set of functionalities and associated protocol operations are required to support, in a common framework, MIHO and NIHO. The architecture presented in this thesis (see chapter 4) specifies modules implemented in the terminal side, in the access part of the network and in the home domain. The mobile device offers a cross layer two/layer three design for wireless/wired technology management, compounded by an intelligent module for interface selection based on several parameters spanning from layer two related information up to user preferences and context aware applications. Protocol communications between the mobile device and the access router (first layer-3 hop in the access network) allow exchange of information for neighbor discovery, handover preparation and handover execution. Handover target selection is done by combining mobility and resource management mechanisms such as admission control. That is, handovers could potentially be denied to mobile devices. To improve performance and avoid as much as possible these situations the architecture further proposes the possibility to initiate handovers from the network upon for instance load detection or conditions changed due to the availability of new access technologies.

Enhanced methods to control user mobility, across these multiple environments, are a requirement for an expected future in which terminals equipped with one or more network interfaces roam across networks, in a multi-diversity of macro and micro wireless cells, the so-called ”4G networks” environment. These mobility methods should consider both traditional terminal mobility (mainly due to user movement), and mobility across heterogeneous networks in novel scenarios, where network load balancing or user context preferences may require mobility triggers also in the network side. To combine these different triggers, there is a need of a cross layer approach, starting from a potentially large diversity of layer two access technologies up to the common IP layer, to exchange messages between terminals and network components. Traditional host mobility driven concepts need therefore to be combined with more stringent mobile operator requirements of network controlled mobility. Thus, users on the move, while enjoying seamless services, can take advantage of optimal mobility choices, eventually mainly computed by network components.

Following this orientation, in the concept behind this chapter we evolve standard mobility mechanisms by adding network intelligence able to i) understand the diversity of layer two wireless cells, and ii) converge new mobility services on top of an IP common layer. In this work, mobility is not regarded anymore as a pure reaction upon terminal movement, but rather as a potential service that future Mobile Operators might offer to customers in different forms and multiple degrees of complexity. Thus, terminal mobility can be either controlled by the network (upon network detection triggers coming from the terminal) or fully initiated from the network (supporting optimizations where required).

The remaining of the chapter is organized as follows. In first place we analyze the benefits obtainable by applying NCHO (section 6.2). These benefits are quantified in terms

of increase amount of users in the system or rejection probability (see section 6.2.3). We also present detailed results of scenarios where the use of NCHO is particularly beneficial (section 6.2.4). The second part of this chapter is devoted to analyze a possible integration of the NCHO concept in the IEEE 802.21 architecture (section 6.3), providing terminal and network entities architectures (section 6.3.5) and performance metrics (see section 6.3.6). Finally we present a summary of the work in section 6.4.

6.2 Network Controlled Handovers:challenges and possibilities

Based on the definition of NIHO and MIHO in the previous sections we present in the following a simulation study by comparing network performance when MIHO and NIHO techniques are applied. NIHO provides improved resource allocation when heterogeneous wireless/wired access technologies are deployed. We aim at quantifying the benefits of this approach and at identifying conditions that affect the relevance of NIHO support. It should be noted that NIHO-related signaling performance per itself is not addressed in this section, we will address this in section 6.3.3.
In this section we focus on scenarios with only one technology, because the benefits of a combined solution of NIHO + MIHO are a lower limit to the benefits achievable using this paradigm. That is, without loss of generality the simulation study focuses on the intra technology case, providing considerations for the framework design at layer three.

Simulation setup

In order to study the performance of NIHO technology a customized simulator, in C++, has been developed. Although this work is centered in inter-technology handovers, processed at IP-level, the design of such a test network, considering multiple technologies (such as WiFi, 3GPP, etc..), with different cell sizes, present simulation problems in terms of channel propagation models, layer-2 protocols, and overall cell interplay. For simulation purposes, we decided to simplify our model being this the main reason for a special-purpose simulator implementation, considering a single technology, and regular cell placements. Thus the reference simulation scenario is composed by six access points deployed in a hexagonal grid. It should be noted that even if we use the term Access Points, the simulator does not contain technology dependent definitions and the scenario presented is valid for any technology mix (provided path loss models are consistent). During the simulations two studies have been performed, please note that both studies are examples of NCHO since in both cases the network has the final decision of accepting or rejecting a handover.

1 First, simulations have been performed in scenarios where MIHO is used. This provides reference results for the scenarios.

2 In a second stage, the simulations combines both MIHO and NIHO techniques, and are then compared with the previous reference results.

In both simulations, Mobile Nodes appear and disappear (corresponding to service calls) according to a Poisson process, with variable frequency (variable system loads). The lifetime of the Mobile Node follows an exponential law with mean 180 seconds, but if no service can

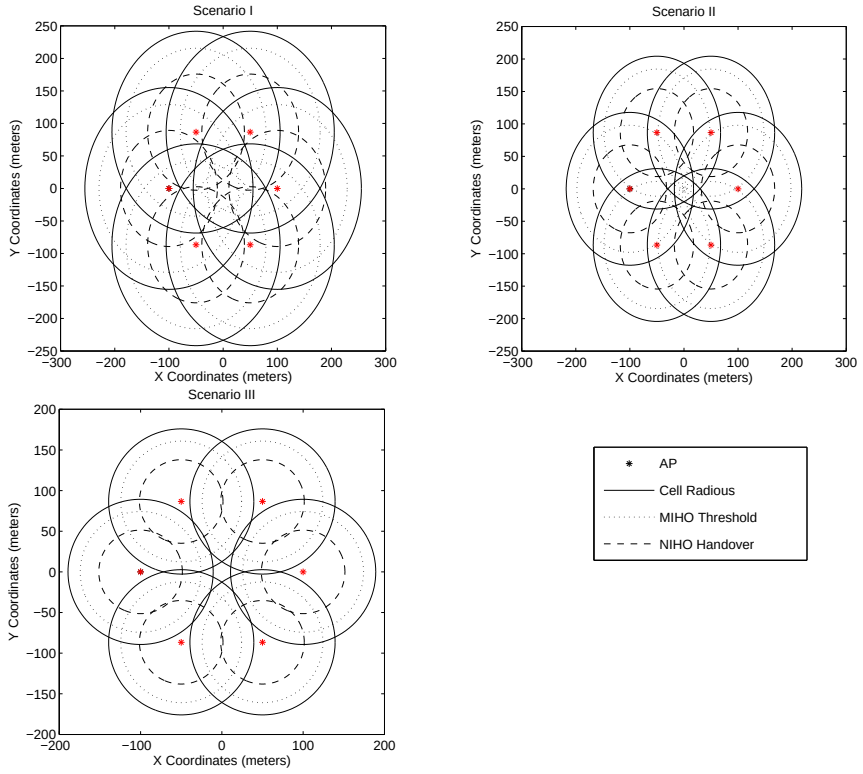


Figure 6.1: From left to right: Overlapping Scenario I, Overlapping scenario II, Overlapping scenario III

be provided (that is, the service call is rejected) the Mobile Node is immediately removed from the system. To cover different types of mobility, the speed of the Mobile Nodes has been selected randomly between 2 and 5 m/s. The Random Way-Point mobility model has been selected for both cases, MIHO and NIHO. During a simulation if the Mobile Node reaches a scenario boundary, the mobility pattern is altered and a new destination target is computed. The maximum number of users per Access Point is set to 10. Results are averaged for 30 simulation runs, taking confidence intervals of the 95% in all the data presented in this study. The Path Loss model used in the simulator is based on the Omnet++ Wireless LAN Path loss model, expressed by equation 6.1.

$$\begin{aligned} Losses(dBm) &= 40 - 10 * \rho Lexp * log(distance) \\ \rho Lexp &= 2.5 \end{aligned} \tag{6.1}$$

Studied Scenarios

To study the impact of wireless overlapping regions on the NIHO performance improvement, three different scenarios were evaluated. Figure 6.1 shows the three scenarios. The difference between them is the wireless coverage area. Each of the Access Points in figure 6.1 shows three different circles: (from out to inside) sensitivity, MIHO and NIHO thresholds.

This set of thresholds is needed since in our analysis we consider very simple algorithms for triggering the handover, based on the load of the Access Points and received signal levels. The algorithms used for NIHO and MIHO and the relation with the thresholds presented above will be explained in sections 6.2.1 and 6.2.2. Threshold values are displayed in table 6.1. These values were selected in order to evaluate all possible cases of overlapping areas for NIHO, leading to scenarios with different characteristics. Scenario I models a system

Threshold	Scenario I	Scenario II	Scenario III
Sensitivity	-90 dBm	-87 dBm	-84 dBm
MIHO	-88 dBm	-85 dBm	-81 dBm
NIHO	-84 dBm	-81 dBm	-78 dBm

Table 6.1: Threshold Values for the different scenarios

with a high number of overlapping areas. Due to this, the results derived from the execution of MIHO should be quite near to the optimal behavior of the system, and probably will not leave much room for system optimization, without complex management algorithms. Scenario II shows a system with an ”average” degree of overlapping areas. In this system, the introduction of NIHO should outperform MIHO-only performance. This is the expected usual scenario. Scenario III corresponds to a (atypical) poor overlapped scenario, where the Access Points do not present an overlapping enough degree to enable system wide optimization. In this case the nodes can only be moved between adjacent Access Points. Moreover, the NIHO overlapping thresholds do not cover the center of the scenario providing a ”hole” in the grid that may produce strange behaviors. We will show that even in the worst case scenarios the usage of NIHO will still be advantageous, improving both Mobile Node service probabilities and overall system performance.

6.2.1 Mobile Initiated Handover Algorithm

For the MIHO study, the Mobile Nodes perform a handover when the MIHO threshold is crossed. In this case the Mobile Node evaluates both the signal and load conditions of every neighboring Access Point. The handover will be performed to the Access Point with the best signal level providing required capacity is available. Notice that we are considering the best case of MIHO, i.e. a MIHO that is performed not only based on information available in the mobile node but also on information provided by the network. The information needed to evaluate the algorithm presented, such as the Access Point’s load, it is suppose to be provided by a framework such as IEEE 802.21. Pseudo code 1 shows the algorithm the Mobile Node executes when reaches a MIHO threshold. A similar procedure is followed when a new Mobile Node is created in the system.

6.2.2 Network Initiated Handover Algorithm

When the combined solution of MIHO and NIHO is applied, the algorithm explained in section 6.2.1 is still applied by the Mobile Node. However, now the network also can move target Mobile Nodes each time a timer expires. The way of moving Mobile Nodes can be potentially implemented according to more complex or simple algorithms. In our case, when the timer expires, all the Mobile Nodes that are inside a NIHO threshold of a target Access

```
for all AP seen by this Mobile Node{
        if load of this AP is lower than MAXLOAD{
                add AP to the Available APs list
        }
}
get AP with best signal from the list of available APs
do handover to the AP with best signal
```

Pseudocode 1: MIHO Algorithm

Point are moved to that Access Point, provided the load is less than the load of the current Access Point the Mobile Node is attached to. In case of having several overlapping NIHO thresholds, the one with best signal level is selected. Note that this NIHO algorithm is quite simple, and results presented are probably a lower bound on overall system performance improvement. The timer on which NIHO depends is one of the critical variables studied during the simulations. Pseudo code 2 shows the algorithm executed each time the timer expires (emulating events report triggering).

```
for all Mobile Nodes{
        get the list of APs which this MN is inside their NIHO threshold
        for all APs in the list{
                if the load of this AP is lower than the load of the current AP
                the MN is connected to{
                        add AP to the Available APs list
                }
        }
        get the AP with best signal from the list of available APs
        do handover to the AP with best signal
}
```

Pseudocode 2: NIHO Algorithm

6.2.3 Metrics and Results Evaluation

The performance metrics analyzed are the following:

- Mean number of users in the system.
- Probability of Rejection at first connection.
- Probability of Rejection while performing handover.
- Decrement in the number of Handovers (Mobile Initiated) between MIHO and MIHO plus NIHO.
- Ratio between Mobile Initiated Handovers and Network Initiated Handovers in the MIHO plus NIHO case.

For each of these metrics, a study on the effect of the degree of overlapping, system load, and the effect of the timer duration has been performed. It should also be noted that all the mobile nodes in the system have the same priority and the same profile i.e. no gold/silver/bronze users are considered, and are generating the same type of traffic. As a general consideration

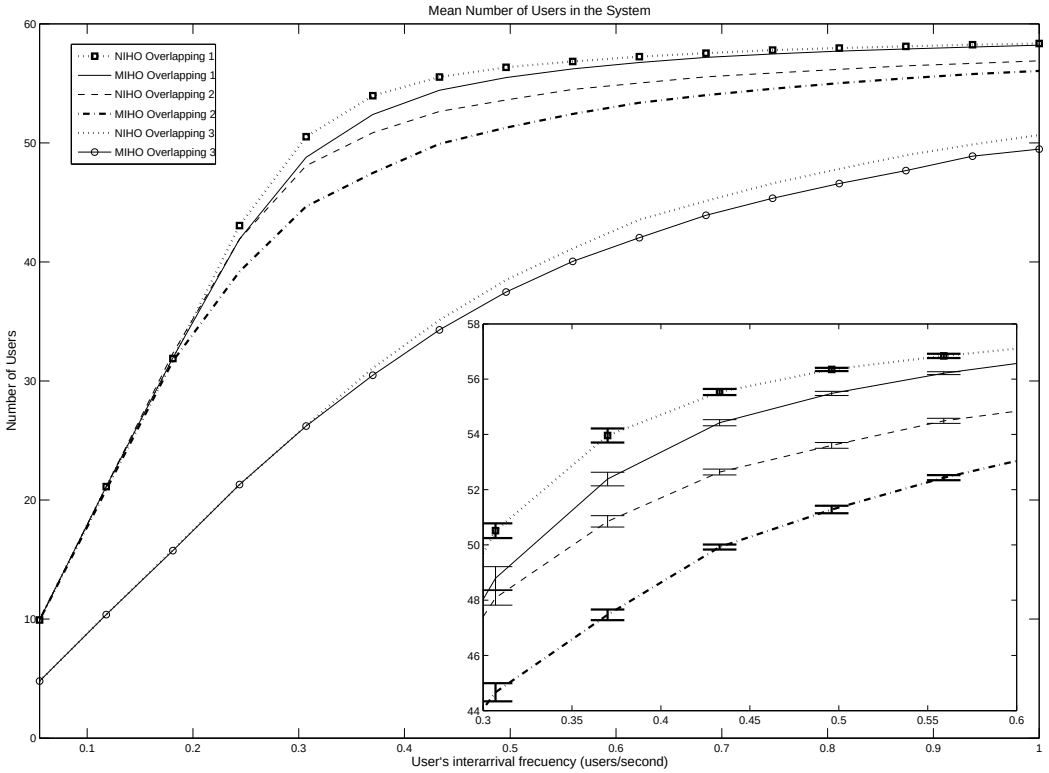


Figure 6.2: Mean number of users

we have to note that, for completeness, the system is also analyzed in saturation conditions. When the system (all the cells) operates close to 100% of the total load, resource optimization techniques (NIHO) are not expected to provide additional benefit, but simulations have been run nevertheless.

Mean Number of Users in the system

Figure 6.2 shows the mean number of users in the system for the three different scenarios depicted in figure 6.1. The maximum number of users depends on the degree of overlapping in the system. In a system with a 100% of overlapping between all the Access Points the maximum number of users in the system is equal to 60. In fact, by decreasing area overlap, the mean number of users decreases as well (since users' mobility becomes constrained). Figure 6.2 shows how the use of a combined solution of MIHO and NIHO produces an increment of the number of users that can be supported by the system. The maximum difference between MIHO and MIHO+NIHO appears in the overlapping II (figure 6.1) and corresponds to just 6%. Although the maximum performance improvement between MIHO and MIHO+NIHO appears for the usual overlapping II case, the maximum number of users in absolute values is reached for the overlapping I. The effect of changing the overlapping area corresponds to a flattening of the curve in figure 2, showing that the maximum number of users is reached with lower frequencies. The maximum number of users reached for the different overlapping areas decreases with the overlapping.

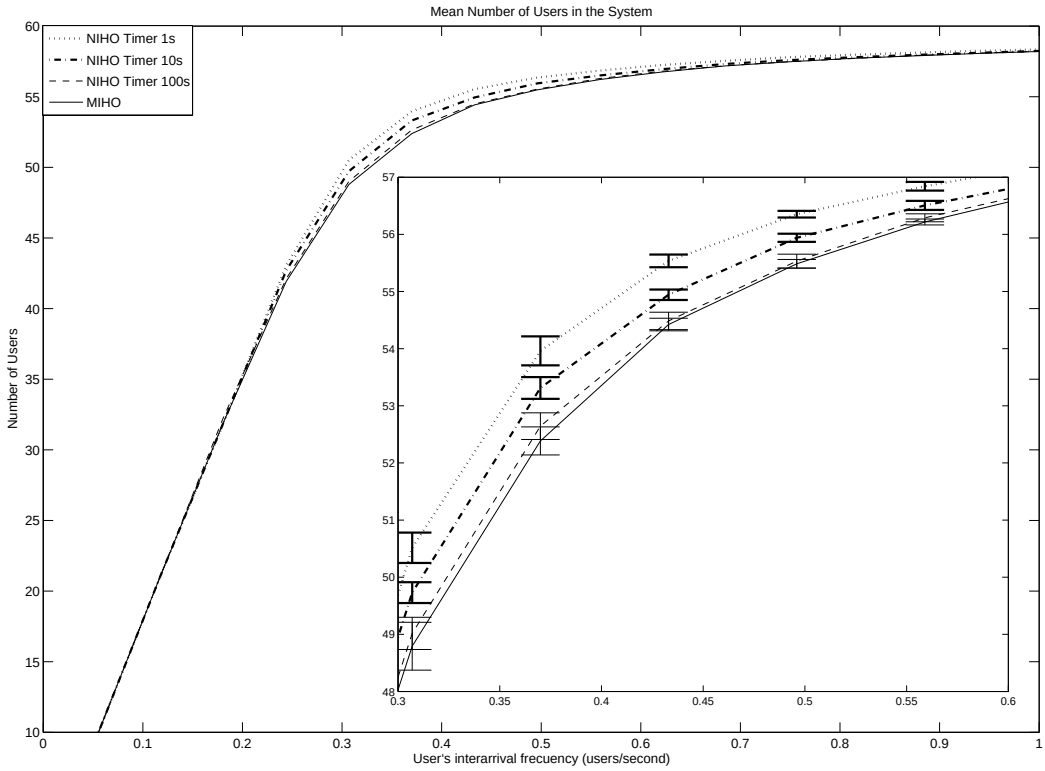
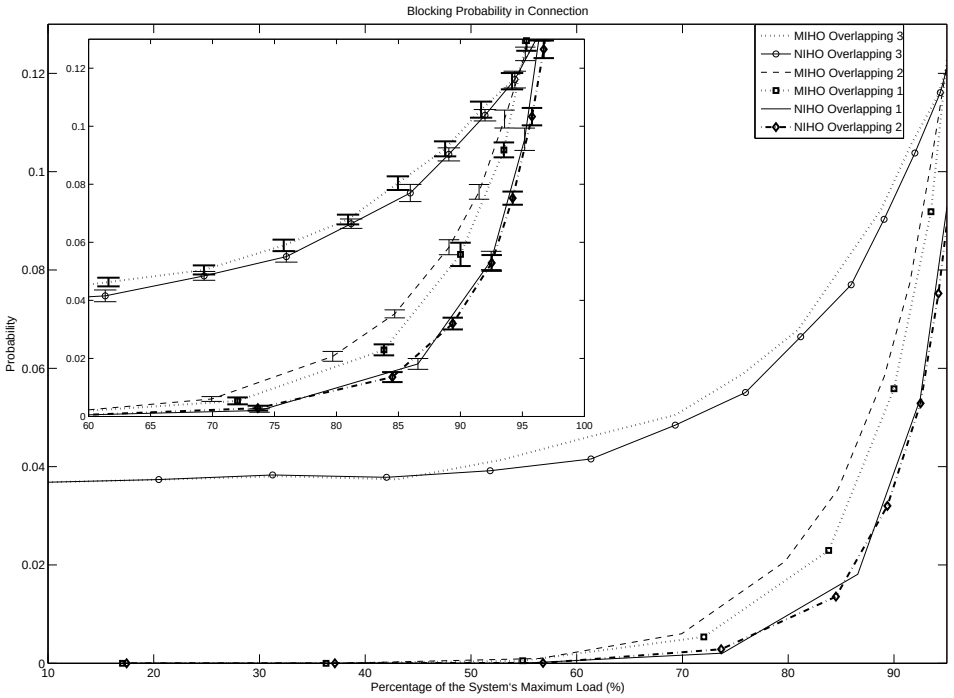


Figure 6.3: Number of users (varying timers)

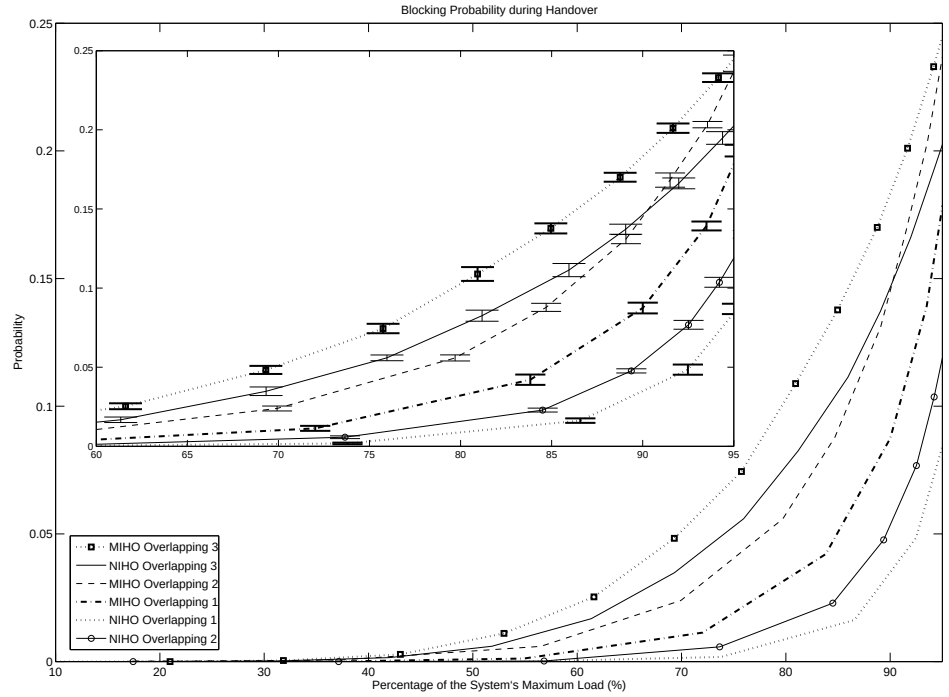
Figure 6.3 shows the effect of increasing the timer which triggers the execution of NIHO. Decreasing the timer does not affect the maximum number of users although the utilization of the system is slightly higher when shorter values for the timer are used. This is due to the fact that, in the case of small inter-arrival times, the system with shorter timers (e.g. more constant optimization updates) supports more users.

Rejection probability in first connection and during a handover

Figure 6.4 shows both the Probability of Rejection at first connection (figure 6.4(a)) and the Probability of Rejection during a handover (figure 6.4(b)) for the scenarios depicted in figure 6.1. The Probability of Rejection at first connection represents the probability of a Mobile Node not finding a free Access Point when arriving at the system. As can be seen, the combined solution MIHO+NIHO decreases this probability when the load starts to reach values higher than 60% of the maximum load in the system. For instance, for the second scenario, heavily loaded (90%), this probability is decreased by 50%. When area overlap is decreased, similar behavior is noticed. The graphs tends to smooth, achieving the form of the graph corresponding to the scenario III as system becomes saturated, and no more Access Points are available. The Probability of Rejection during a Handover represents the probability of the handover being rejected due to admission control when the Mobile Node is performing a Handover. In this figure we can see how the probability decreases always when MIHO+NIHO are used, and the difference is appreciable for loads higher than 60%.



(a) Probability of Rejection in first connection



(b) Probability of Rejection during a Handover

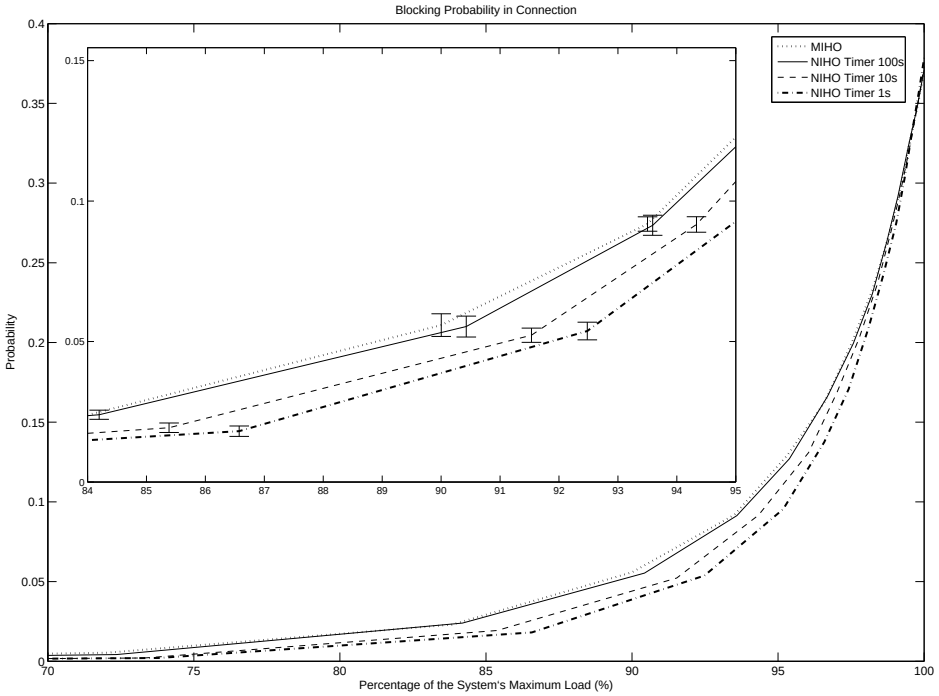
Figure 6.4: Probability of Rejection

In the case of load 90% the second scenario is decreasing the rejection probability in 64%. The effect of the overlapping on the Probability of rejection during a handover, is to increase the blocking probability while decreasing the overlapping. This is due to the fact that as less overlapping exists in the system, the load balance mechanism works worse, so the Access Points have higher loads and the blocking probability in connection increases. The same effect can be observed in the blocking probability during a handover. It is worth to notice the important reduction in the probabilities achieved using MIHO+NIHO, although the number of users is increased by a 6%, the probability of rejection in connection is decreased in a 50%. Being this decrement in the probability and increment in the number of users, very important from the operators' point of view.

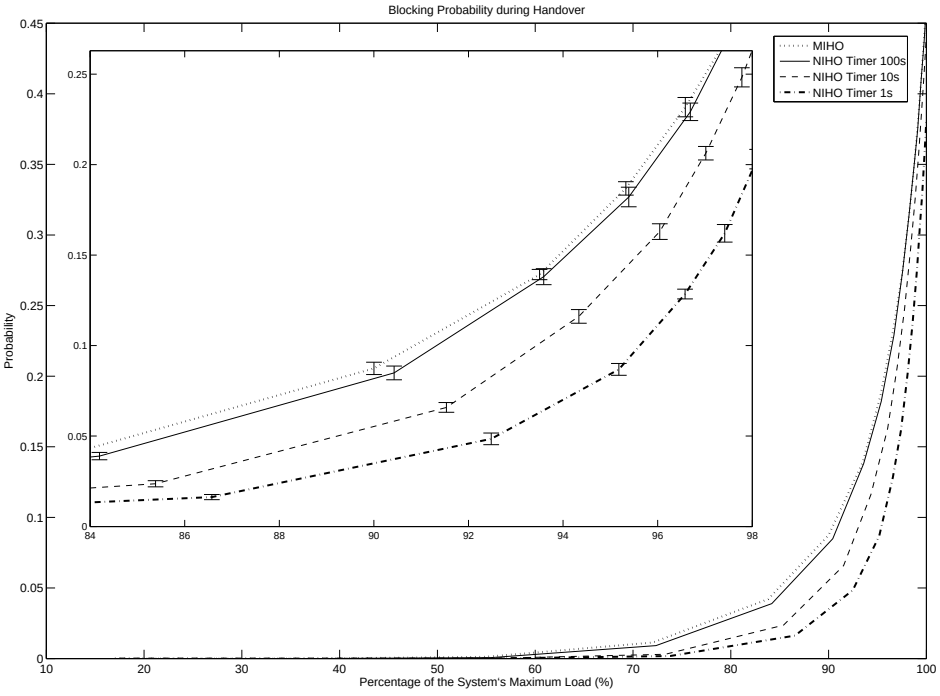
Figure 6.5 shows the effect on the Blocking Probabilities at first connection (figure 6.5(a)) and during a handover (figure 6.5(b)) for variable NIHO timer values. As can be seen the effect of increasing this timer corresponds to increase the probability of blocking in both situations, bordering the MIHO behavior when the timer is very long (100 seconds).

Number of Handover Operations

Figure 6.6 shows the metrics related with the number of handovers performed. These two graphs show the NIHO impact from the perspective of the user and of the network. The decrement in the number of Handovers shows how the Network Initiated handovers are decreasing the number of Mobile Initiated handovers due to mobility. This decrement shows that the NIHO algorithm used always improves the receiving situation of the Mobile Node, by moving it in a position where the probability of doing another handover due to signal conditions is lower or equal than in the previous situation. As in the previous graphs, the percentage of decrease depends on the load of the system and as it increases the performance of the combined solution NIHO plus MIHO decreases. It is worth to notice the important reduction in the number of handovers due to mobility that occurs for the first scenario, where in the best case a 28% of reduction is achieved. As the overlapping decreases the reduction in the number of handovers also decreases. This is due to the fact that there is less area where NIHO is performed. In the case of the third scenario, it can be seen that the decrease in the number of handovers is more or less constant, and to some point independent of the load in the system. This effect appears due to the fact of the small area that NIHO covers. As the area is smaller, the effect of NIHO is diminished providing only movement between adjacent Access Points.
The Ratio between Mobile Initiated Handovers and Network Initiated Handovers presents the relative cost of applying NIHO to the system. It represents how much the total number of handovers is increased when NIHO is applied. As can be seen, for the scenario I the peak is situated in 1.5, which means that the total number of handovers in the reference scenario is multiplied by this quantity while using NIHO. As happens in all the other graphs, as the system is saturated this ratio decreases because the possibilities of moving a node when the system is saturated decreases. As the overlapping changes this ratio decreases because Network Initiated handovers are performed with a greater difficulty. Figure 6.7 presents the effect in the metrics related with the number of handovers when the timer is increased. As expected the Decrease in the number of Mobile Initiated Handovers is reduced while the timer is larger. This effect is similar in behavior as when the overlapping is decreased. As



(a) Probability of Rejection in first connection (varying timers)



(b) Probability of Rejection during a Handover (varying timers)

Figure 6.5: Probability of Rejection (varying timers)

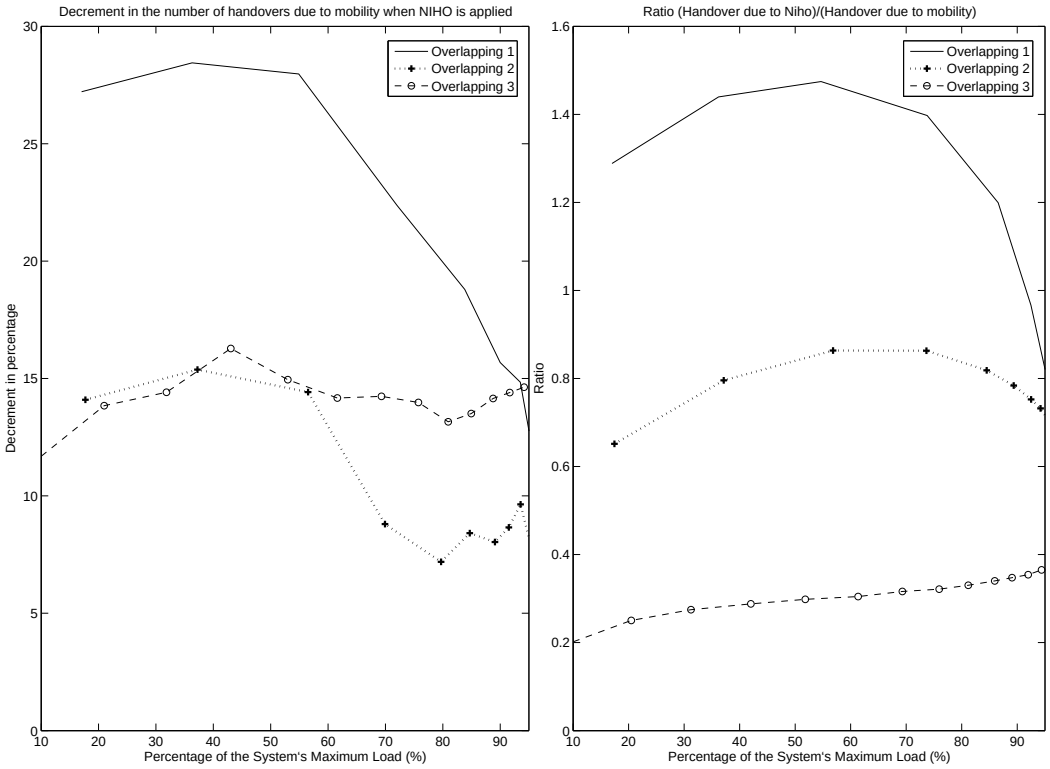


Figure 6.6: From left to right: Decrement in the number of Handovers (Mobile Initiated) between MIHO and MIHO+NIHO, Ratio between Mobile Initiated Handovers and Network Initiated Handovers in the MIHO+NIHO case

the timer is larger the number of Network Initiated handovers is less and the Mobile Nodes are situated in the area of influence of NIHO less frequently. The Ratio between Mobile Initiated Handovers and Network Initiated Handovers presents the same effect decreasing with the load of the system and with the duration of the timer.
Through these results we argue that the use of NIHO in the network is providing an interchange between handovers performed by the terminal and handovers performed by the network. As has been proved, when the NIHO effect is greater the number of handovers due to mobility decreases and the number of handovers performed by the network increases. Although it could seem that this interchange does not provide any benefit to the provider, is worth to notice that the handover performed due to mobility reasons tend to be unstable in signal level, with a higher probability of disruption in the communication. The handovers performed by the network are done always in good signal conditions and as they are network controlled, the probability of disruption in the communication is lower. Although the same effect could be obtained by reducing the thresholds while performing a mobile initiated handover, the fact that the network is controlling the handover gives several benefits for QoS and load balance that cannot be achieved with mobile initiated handover mechanisms.

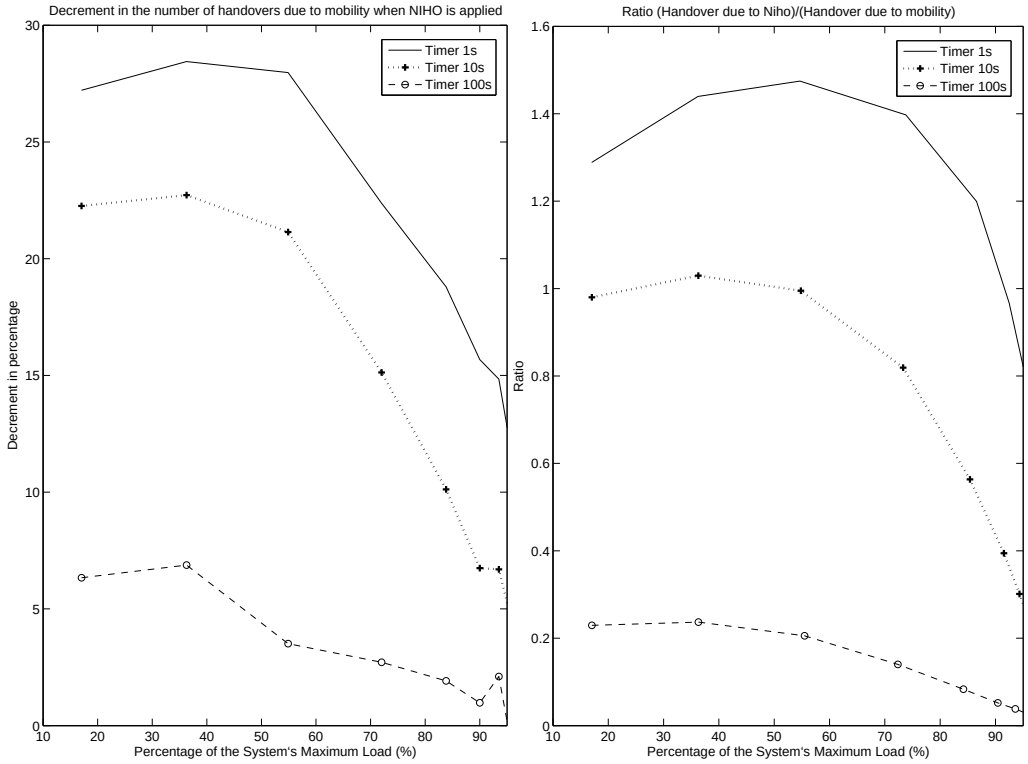


Figure 6.7: From left to right: Decrement in the number of Handovers (Mobile Initiated) between MIHO and MIHO+NIHO, Ratio between Mobile Initiated Handovers and Network Initiated Handovers in the MIHO+NIHO case (varying timers)

6.2.4 Increased advantage of using NIHO in asymmetrical scenarios

Last section presented simulation results considering evenly distributed mobile nodes over a limited region with different wireless overlapping cells. The mobile nodes are uniformly distributed and are dropped from the network as soon as the terminal is denied connection, either because of rejection during handover or because of rejection at first connection. These are reasonable assumptions when studying the performance of the network trying to understand what are the blocking probability values of the system under evaluation. However, to present the full potential exploitation of the NIHO technology we have to introduce some more specific cases where distribution of the nodes is not uniform. In fact, this is a common situation in some scenarios where physical conditions create concentrations of users (e.g. airports). Another situation with the type of asymmetrical distributions in which NIHO can provide increased benefit is the multi-technology case, where the asymmetry is created by the different characteristics of the technologies.
The scenario analyzed considers mobile nodes generated with higher probability in the same region, thus leading to an overload of certain access points. In this new scenario the overlapping regions allow the network to move terminals around, aiming at redistributing the load and increasing the network capacity. It should be noted that without NIHO technology the network would be overloaded only in some portions and the rejection

probability (mainly because of admission control) would increase beyond acceptable values. The necessary condition to avoid this is a good planning of the overlapping area across technologies. If we consider simply a single wireless technology, this overlapping is strictly related to physical channels availability, whereas in case of heterogeneous wireless technologies the overlapping cells planning can become more complex. In both cases the overlap percentage should be sufficient to move terminals to another cell while keeping (if not improving) similar link characteristics. This can be implied by the results in the previous section.

To check experimentally that NIHO achieves an increased performance benefit in situations with asymmetrical distribution of nodes, we analyze the following scenario. We have a set of three access points with sufficient overlapping area. Each access point is able to accept at the maximum 10 mobile nodes (admission control).

To simulate a real life environment we let mobile nodes always being generated in the middle access point area. Movement is allowed within the overlapping area never leading to disconnected terminals. This is a realistic scenario, for instance, in airports where people getting off at the gate switch on their mobile devices while leaving the plane. In such case mobile users generate extra load in the middle access point tending to saturate the system and increasing the rejection rate for people newly connecting to the network. It would be desirable to have intelligence implemented in the network able to react upon a configured threshold and instructing mobile nodes to connect to alternative access points. The scenario provides insightful results on how overlapping should be configured to allow network intelligence to perform NIHO, even across multiple technologies.
The decision algorithm implemented is as follow. Besides the timer based control, the algorithm (pseudo code 2) is also triggered when the NIHO LOAD THRESHOLD is crossed (set to 5 in the simulations). This simple but efficient mechanism shows the effects of the NIHO technique on the previously introduced metrics.

λ	NumberUsers	RejectHOProb	RejectConnProb	NumberHO	Load
0.04	9.53%	83.2%	86.78%	14.16%	50.52%
0.06	7.64%	85.57%	85.6%	16.57%	63.9%
0.12	24.9%	64.73%	55.04%	84.8%	84.7%
0.31	30.52%	28.12%	44.8%	14.93%	92%
1	31.15%	9%	21.8%	56.13%	100%

Table 6.2: Metrics values for different network loads (lambda)

The results are summarized in table 6.2. The first column (*"λ"*) indicates the user inter-arrival frequency used to increase the load in the network following a Poisson law (mean connectivity to the network is fixed to 180 seconds). The second column, (*"NumberUsers"*) indicates how much in percentage the number of users is increased in the same scenario when NIHO+MIHO is applied compared to pure MIHO only. The third and the fourth columns (*"RejectHOProb"* and *"RejectConnProb"*) indicate the decrement (in percentage) respectively of the reject probability during handover and the reject probability at connection. The fifth column (*"NumberHO"*) represent the percentage of reduced number of handovers trig-

gered for mobility reasons. Finally the last column (*"Load"*) represents the load of the system for the lambda used.
The results show that the total increment of users, when NIHO is applied, is around a 30%. Probability of rejection during handover and at connection time is reduced, confirming the tendency already presented in the previous section. It is worth to notice how using NIHO+MIHO the number of users is incremented while the probabilities of rejection during a handover and at connection are reduced, showing a clear benefit for operators. We argue these results clearly show the benefit of NIHO techniques, being this kind of scenarios likely to happen in open environments such as airports, shopping malls, public hotspots. Mobile operators have therefore the possibility to better control terminals in the network and potentially increasing the number of users consuming services. That is, the technology opens new business and revenue opportunities for mobile/fixed operators.

6.3 Toward IP Converged Heterogeneous Mobility: A Network Controlled Approach

On the previous section (section 6.2) we have analyzed the potential of network controlled handovers (NCHO) to increase the performance and resource usage of the network. In this section we further study the NCHO concept by providing design considerations and proposing a framework for the integration of NCHO on IEEE 802.21 capable networks.

The IEEE 802.21 (or Media Independent Handover (MIH)) technology is an enabler for the optimization of handovers between heterogeneous IEEE 802 systems as well as between 802 and cellular systems. The goal is to provide the means to facilitate and improve the intelligence behind handover procedures, allowing vendors and operators to develop their own strategy and handover policies. Furthermore, IEEE 802.21 is potentially usable in multiple mobility scenarios, both mobile and network initiated, and it is independent of the location of the mobility management entity.

Figure 6.8 depicts the 802.21 communication model with functional entities and associated interfaces, where the MIH technology is implemented in the mobile nodes and network side components, both being MIH-enabled. For more information related to IEEE 802.21 or its reference model (figure 6.8) please refer to chapter 2.

For analyzing vertical handovers between WLAN and cellular systems, our framework exploits the communication exchanged over interface R3, implementing the necessary events and command services for link detection and handover initiation and execution. As stated in section 6.3.3 (where an accurate analysis of the required packet sizes is reported) we argue that the cost in terms of bandwidth to implement such interface is negligible with respect to data traffic flowing from/to the terminal.

Our control plane for optimized vertical handover management exploits IEEE 802.21, but is complemented by the Mobile IP (MIP) protocol. MIP provides Internet connectivity to mobile nodes roaming from one access router to another, regardless of the access

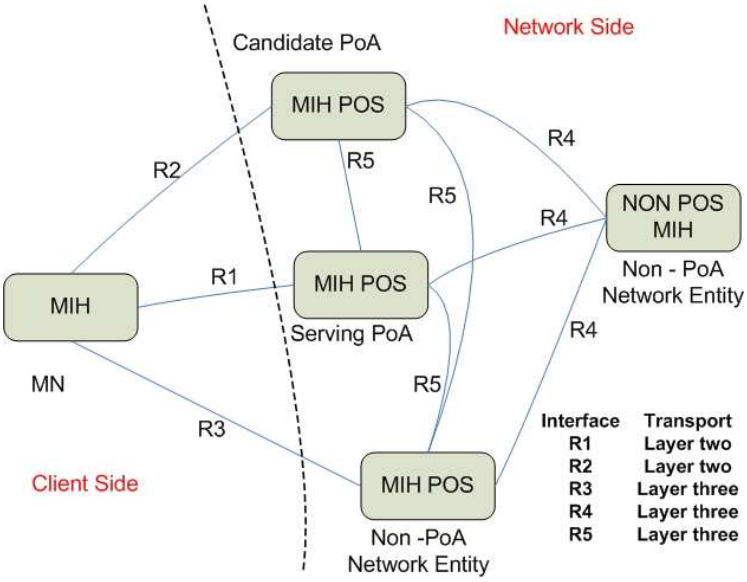


Figure 6.8: IEEE 802.21 Communication Model

technology supported in the router.

From an IEEE 802.21 viewpoint, MIP (as a Mobility Management Entity in the mobile node) can be regarded as a high-level entity which uses the services provided by the MIHF layer, i.e. it is a MIH-user. These services include, amongst others, the means to control L2 handover initiation and attachment, as well as link layer events that can be used as triggers to initiate the L3 handover procedures.

6.3.1 Framework Design

As mentioned above, our framework exploits the R3 (IP based) interface in IEEE 802.21, between the MN and the PoS (central entity), integrating the control signaling with Mobile IP signaling for data plane update. For simplicity (and due to its current industry relevance) we will discuss our proposal only applied across WLAN and cellular technologies.

In our scenario, global coverage from cellular technologies is always available, and enhanced coverage is available in multiple WLAN hotspots, a common situation currently. The mobile terminal typically performs a soft-handover (meaning that the new link is established before releasing the old one) between different interfaces, although our framework could be adapted to hard-handovers (in which the connection is set up through the new interface after closing the previous one in use). This framework defines two network operational modes, which play the same role as the ones defined in section 6.2. In both cases the handover decision is taken by the network, so both modes are cases of Network Controlled Handover (NCHO), as defined in section 6.2. Namely the operational modes are i) Mobile Initiated and ii) Network Initiated and Mobile Assisted.

Mobile Initiated

This operational mode places the handover initiation decision in the Mobile Node (MN). When the MN reaches a WLAN cell and estimates there are favorable conditions, it will inform the network (PoS) of the new link detected, waiting for a confirmation from the network which allows or denies the execution of the handover procedure. This way the final decision of performing a handover is taken by the network.

The analysis of Mobile Initiated Handovers will then assess the impact of the proposed IEEE 802.21 signaling compared to old scenarios of pure host driven mobility, which do not have the overhead of decision making signaling and no network cost exist. For more information regarding Mobile Initiated handovers not controlled by the network, please refer to chapter 5.

Network Initiated and Mobile Assisted

This operational mode places both the handover decision mechanism and the handover initiation decision in the PoS. The MN assists the handover decision mechanism by providing measurements of the environment where it is currently situated. This operational mode has been studied considering the impact of signaling on handover performance (as in the previous operational mode). The analysis of network controlled and initiated handovers will then show how network decisions can impact terminal mobility, and which associated functionalities are required for these operations.

6.3.2 Signaling flows

Figure 6.9 presents the IEEE 802.21 signaling flow developed to perform a handover. This signaling is explored in both operational modes, with small differences. The detailed list of parameters included in each message is presented in subsection 6.3.3.

3G⇒WLAN Handover

The signaling flow for the 3G⇒WLAN handover supposes a MN that is connected to 3G and is approaching a WLAN cell (figure 6.9). The scenario considers a mobile node connected to a 3G link, crossing zones where Access Points are present, allowing for vertical handover opportunities. We focus on a single PoA (AP) per vertical handover opportunity, in a scenario featuring multiple PoAs.

As soon as an access point (AP) is detected as result of the Active Scanning procedure, the MIH Function at the MN receives a corresponding indication from the link layer and sends message (1) to the PoS, encoding the MAC address of the AP in a UDP packet. This message is followed by message (2), where information related to the change in signal strength is supplied to the PoS. The PoS is then able to verify information related to that target, such as the load value. In the same way, Access Points (or PoAs in this scenario) are able to provide link events, via 802.21, indicating their load value to the PoS. In this way, the PoS is able to have an up-to-date information about the load of the PoAs, and use this information as an input to the handover decision. Upon load evaluation (3) at the PoS, message (4) is received in the MN, which replies with message (5), informing if the handover is possible or not. Note

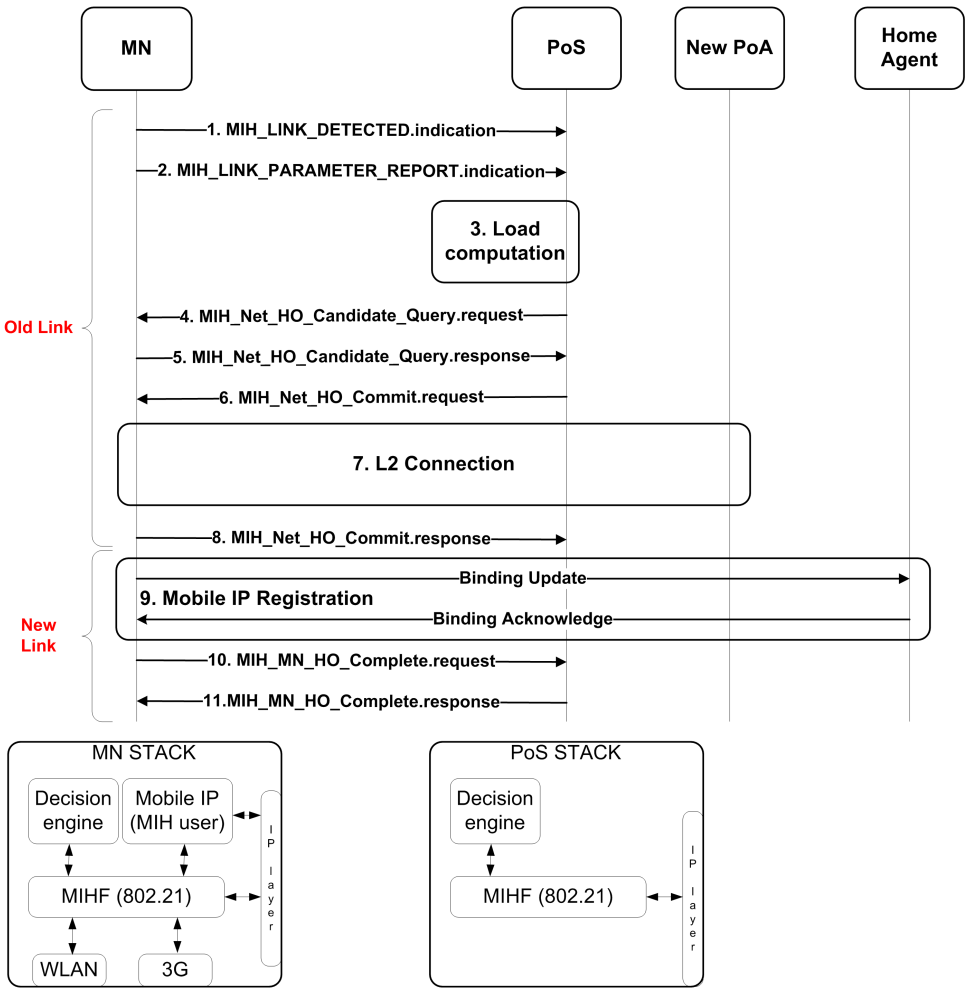


Figure 6.9: Handover Signaling for WLAN⇒3G and 3G⇒WLAN handovers

that the handover target in the handover request might not correspond to the one the MN is located at, in case of network handover initiation (e.g. because of terminal mobility). The PoS, upon reception of this message, sends message (6). The MN processes this datagram in the MIHF, sending a local link command to the wireless interface, in step (7) to start the L2 association procedure. In this case, the standard IEEE 802.11 association state machine is used, because this is a WLAN association. However, an important factor to retain here is that the network PoS is able to issue a remote 802.21 command towards the mobile node, an that command is translated by the MIHF into a specific technology command. In this case it is 802.11, but it could be 3G, 802.16, etc. Upon successful L2 association[1], message (8) is sent to the PoS. If the signal strength conditions are still favorable, the MN can execute a L3 handover (9) (a MIP registration) through the new link. Upon successful MIP registration, message (10) is sent to the PoS, which replies with message (11). Finally the MN is able to

[1]Please note that in the simulator an active scanning procedure has been implemented to guarantee favorable radio conditions.

receive L3 traffic as result of the MIP binding procedure. Note that the difference between a soft and hard handover is only related with the moment when data is not further received through the old link, and does not affect the signaling flow.

WLAN⇒3G Handover

This case supposes a MN associated to an AP, and the MIH Function continuously evaluating the signal level supplied by beacon messages. When the WLAN⇒3G threshold value is crossed, the MIH sends a MIH_LINK_PARAMETERS_REPORT (2) to the PoS, indicating deterioration of the received signal level. This will start a signaling exchange with the same messages and sequence as the 3G WLAN handover, except for (1) MIH_LINK_DETECTED that is omitted, since the 3G leg[2] is assumed always active (i.e. PDP context always active).

6.3.3 Signaling Overhead

Given our reliance in 802.21 signaling for the network operation, it is required to evaluate the associated signaling overhead. IEEE 802.21 specifies a set of messages exchanged between the network and the terminal in order to perform a handover. The 802.21 frame is composed by header and payload. The header consists of two parts: a fixed header which carries information related to the type of message and entity which is addressed to, and a variable header which helps in parsing the content of the payload. The first part is always present in any 802.21 message and has a fixed length of 8 bytes, while the second part carries information such as Transaction ID, Session ID or synchronization information and has a variable length.
In our study we suppose that the variable header is always present in the messages (worst case assumption) and its size is 8 bytes. The 802.21 message is completely defined in the payload, which is situated after the variable header. Inside the payload block, TLV encoding is used and the size of the payload block could be variable depending on the message and the parameters used. For each parameter, 5 more bytes should be added in order to complete the TLV format. Alignment to 32 bits is done by means of padding.
Table 6.3 specifies the messages and all parameters used in this study, with the respective sizes of each parameter. Although there is not any transport protocol defined yet for 802.21 datagrams, there are proposals that use UDP [9] (general design considerations are given in [10] based on a common set or requirements [8]). In our framework all the signaling has been performed over UDP/IPv6. For each packet a calculation of the packet size has been performed in the following way:

$$Length = IPv6 + UDP + FixedHeader + VariableHeader + TLV\ params \tag{6.2}$$

The signaling messages per handover sum 672 bytes, from which, in the case of 3G to WLAN, 528 bytes correspond to signaling deployed through the 3G and 144 bytes correspond to signaling through the WLAN. In the case WLAN to 3G the numbers are reversed.
To get an understanding of the cost in terms of signaling when using 802.21, several calculations of the bandwidth used for signaling have been performed, taking into account the

[2]The 3G leg means the 3G part of the network, more concretely, the network point of attachment where the terminal connects to the 3G technology. This term is commonly used in 3GPP specifications.

MIHF Protocol Message	Parameter Name	Type	Size
MIH_LINK_DETECTED	Link ID	Network type	4
	MacNewPoA	MAC Address	6
MIH_LINK_PARAMETER_REPORT	LinkParameterType	Link Quality Parameter Type	1
MIH_Net_HO_Query.request	Handover Mode	Handover Mode	1
	SuggestedMacNewPoA ID	Mac Address	6
	CurrentLinkAction	Link Action	4
	SuggestedNewLink ID	Network Identifier	4
MIH_Net_HO_Query.response	Handover ACK	Handover Mode	1
	Preferred Link ID	Network Identifier	4
MIH_Net_HO_Commit.request	NewLink ID	Network Identifier	4
	NewPoAMAC	Mac Address	6
	CurrentLinkAction	Link Action	4
MIH_Net_HO_Commit.response	OldLinkAction	Link Action	4
MIH_MN_HO_Complete.request	Handover Status	Status	1
MIH_MN_HO_Complete.response	ResourceStatus	Resource Retention	1

Table 6.3: Messages and associated parameters (size in Bytes).

handover probability of our model. Studies like [90], argue that the average number of users in a 3G cell varies up to 52 users. For different numbers of users, the bandwidth used for signaling can be calculated and is depicted in table 6.4.

In this table, it can be seen that the signaling load increases with the number of users and

	2m/s		5m/s		10m/s	
N° User	WLAN	3G	WLAN	3G	WLAN	3G
20	6.6±0.6	24.4±2.2	27.7±1	101±3	40.9±2	150±7.6
40	13.3±1.2	48.8±4.5	55.3±1.9	203±7	81.9±4.2	300±15

Table 6.4: Signaling Bandwidth cost in Bytes/sec in function of mobile node speed in m/sec

their speed of movement, but in all cases, signaling load remains very low. In the worst case (40 users moving at 10 m/s) the required signaling corresponds to 300 bytes/second in average, delivered through the 3G link; and 82 bytes/second, delivered through the WLAN. This result corresponds to handovers from 3G to WLAN. The inverse case (WLAN to 3G) has similarly corresponding values.

We argue that the signaling specified in IEEE 802.21 is loading the network very lightly and is enough to support a high number of users performing handovers between different technologies like WLAN and 3G. This supports our intention of exploiting 802.21 MIH functionalities to aid heterogeneity mobility.

6.3.4 Simulation Setup

In this section we present the simulation environment used to evaluate our framework, which also requires the detail of some of the entities involved in mobility management. Our study was conducted by simulating the movement of a MN attached to a 3G network and performing several handovers between 3G and WLAN hotspots, varying terminal speed and coverage threshold values.

The simulation scenario considers wide space with indoor characteristics (such as an airport) in which the user can move at different speeds and it closely follows the network scenario mentioned in section 6.3.1. It consists of an environment with a partial area of non-overlapping WLAN cells[3] and full coverage of 3G technology. The WLAN coverage is supplied by Access Points, each connected to an Access Router. The scenario also features a Home Agent for the MIP Registration process, an audio server which streams audio traffic to the MN[4], and the PoS which is the central network entity that exchanges MIH messages with the MN. This adds the network part of the IEEE 802.21, under standardization, to our model, thus creating a framework suited to model Network Initiated and Assisted handovers. Through the rest of this section several details of the model and the specification of the algorithm which conform the PoS and MN behavior, are provided.
This simulation scenario is similar to the one presented in section 5.3 with the difference that in those contributions only Mobile Initiated Handovers, and without any network control, were considered. As a consequence there was neither the concept of central entity (the PoS) controlling mobility, nor IEEE 802.21 signaling over the air between the mobile node and the network.
The OMNeT++[5] simulator was selected as the primary tool for this study, with each simulation run for 60 random seeds. This number was chosen as a tradeoff between simulation time and confidence interval size. As for the IPv6 neighbor discovery configuration default host/routers parameters values according to RFC 2461 [27] have been adopted. With respect to the WLAN layer two attachment characteristics the simulation considers the typical IEEE 802.11 association state machine, where a layer two association/handover lasts approximately 220ms.

Movement Pattern

The movement pattern selected is the Random Waypoint Mode. The MN moves between uniformly distributed waypoints, at speeds of 2m/s, 5m/s and 10m/s targeting to model speed scenarios that will be the usual worst case in WLAN environments, including the border between WLAN and 3G (the focus of our simulations).

WLAN Model

The WLAN Model used is the one implemented in OMNeT++ based on free space losses with shadowing and a variable exponential coefficient. Each simulation was run with 3G⇒WLAN and WLAN⇒3G thresholds varying between -75dBm and -65dBm.

The 3G Channel Model

The 3G channel has been modeled as a PPP channel with a connection time of 3.5 seconds, disconnection time of 100 ms, bandwidth of 384 kbps (downlink) and variable delay of 100 to 150 ms per way[6]. Although the above model takes into account the connection time,

[3]The setup features four access points distributed in a square area of 500X500 meters.

[4]The traffic studied is a downstream audio, with a packet size of 160 bytes at application layer and inter-arrival packet time of 20 ms (83 kbps). Notice that usual VoIP codecs generate bit rates around 80 kbps and therefore their traffic pattern is very similar to the simulated one.

[5]http://www.omnet.org

[6]Measurements have been taken with a commercial 3G data card.

in our simulations we have assumed that the PDP context is always active, so the value of the connection time does not have any impact. Indeed, our simulations are based on the following two assumptions i) full 3G coverage and ii) 3G link always on, which we argue that are realistic assumptions in typical scenarios.

Metrics used in the study

The main focus of our simulation work in this paper is to verify that the introduction, in a threshold based handover algorithm, of the IEEE 802.21 signaling that enables network control, does not hinder the ability to achieve a good use of the wireless cells. For exploring this issue we used the following parameters:

- Mean percentage of L2 handover without MIP registration (failed handovers)
- Mean number of 3G⇒WLAN handovers
- Mean number of WLAN⇒3G handovers
- Mean wireless utilization time

Regarding the first metric, a failed handover is a situation in which the mobile node detects the WLAN cell and starts the signaling procedure in figure 6.9 but, after receiving message 6 the signal level never goes over the 3G⇒WLAN threshold, and the procedure is not completed, in particular a layer three registration to send the traffic to the WLAN interface does not take place. Notice that this situation does not imply any connectivity problem, as communication continues normally using the other interface. The second and third metric are related to the mean number of 3G⇒WLAN and WLAN⇒3G handovers, respectively. Lastly, we also account for the mean wireless utilization time.

6.3.5 Extended Terminal Architecture for NIHO support

The terminal's architecture includes a subset of the Media Independent Handover Protocol defined in [1]. In this work we focus on the impact of the required signaling to perform handovers while mobile terminals move at different speeds, thus MIH capability discovery and remote registration are supposed to already have occurred.
The handover algorithm reacts to events resulting from the analysis of the signal strength in the WLAN interface (see section 5.2.3). A MIH implemented in the MN supplies triggers to a local decision engine, based on 3G⇒WLAN and WLAN⇒3G thresholds, possibly resulting in a handover. In this paper we complement this algorithm with MIH signaling between the terminal and the PoS. Figure 6.10 depicts the intelligence residing in the MIH layer at the MN. The figure explains how the MIHF residing in the mobile node reacts to link layer events and remote MIH commands received from the network. The events are used to convey up-to-date link behavior to the network decision point, enabling it to acquire information regarding the terminal's point of view of the network. Next follows an explanation of these events and commands, following the order in figure 6.9.
These events are

1. LINK_DETECTED indication when the terminal detects a new WLAN cell.

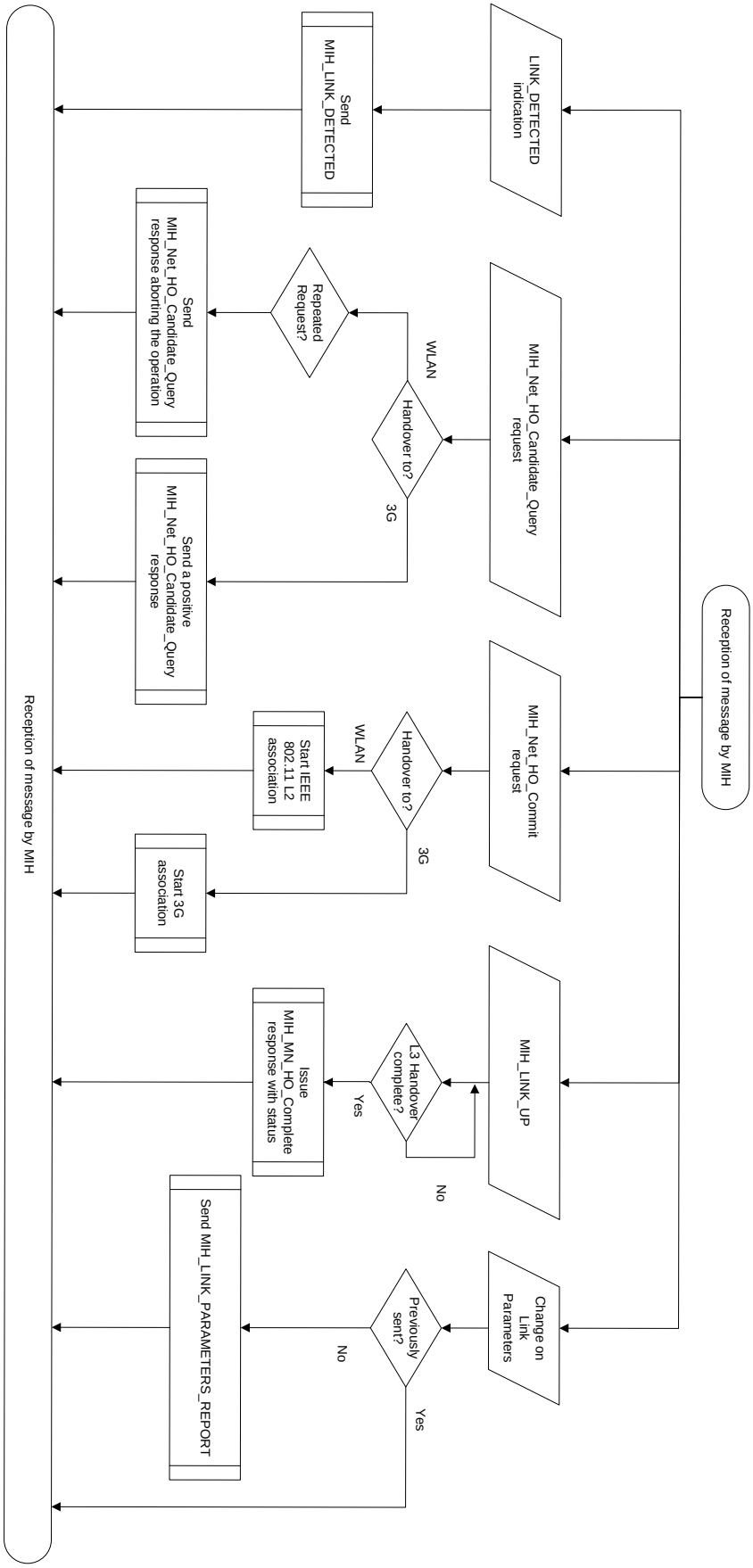


Figure 6.10: MIH Intelligence at the MN

2. Change in Link Parameters, when the received signal level crosses a configured threshold.

3. MIH_LINK_UP that indicates a successful L2 connection establishment.

In case of a change in link parameters, a safeguard was implemented so that a MIH_LINK_PARAMETERS_REPORT event is only sent once per threshold crossing. The rationale for this is that, prior to attachment, the terminal is actively scanning the air medium and continuously verifies the signal conditions of the detected point of access, which would result in a large overhead of MIH_LINK_PARAMETERS_REPORT messages over the air. After reception of these events in the MIHF, they are conveyed to the PoS using the 802.21 protocol message format. In the same way, MIH commands are sent by the PoS towards the mobile node. These commands are received and analyzed by the MIHF and can be

1. MIH_Net_HO_Candidate_Query requesting the mobile node to initiate handover procedures, either to a WLAN or 3G cell.

2. MIH_Net_ HO_Commit requesting the mobile node to execute the required link procedures to commit to the initiated handover.

In case of MIH_Net_HO_Candidate_Query, the MIHF verifies the link type (WLAN or 3G) and, in case of WLAN, if this is a repeated MIH_Net_HO_Candidate_Query command. In both cases, the result is a MIH_Net_HO_Candidate_Query response message towards the PoS, indicating if the handover is feasible or not. In case of MIH_Net_ HO_Commit, the MIHF issues a link command (specific to the handover target technology) to initiate the L2 attachment procedures. After these procedures are finished, a MIH_LINK_UP is received in the mobile node's MIHF from the link layers. This trigger is used to send a MIH_Net_ HO_Commit response towards the PoS, indicating that the L2 handover was successful, and also as an internal trigger to initiate the L3 handover procedures. Finally, when these procedures are done, an indication that the handover is finished is collected by the MIHF, which will produce a MIH_MN_HO_Complete message that is sent towards the PoS, informing it of the handover success.
Due to the configured 3G⇒WLAN threshold, and also to the movement of the node and the delay caused by the signaling, a layer two handover might not lead to a Mobile IP registration (this is one of the metrics of our simulation model, which is extensively studied in section 6.3.6). Since we analyze inter-technology make-before-break handovers, the MN will attempt to establish the new link before releasing the old one. When the MN is connected to the WLAN, and the MIH Function verifies that the received signal strength is not favorable anymore, a WLAN⇒3G is triggered. Thus, the MN starts the MIH signaling to the PoS, potentially initiating a handover to the 3G leg.
While evaluating the more suitable algorithm for the MN, we decided to perform the MIH signaling once the MN reaches the WLAN cell. Thus, when the signal level crosses the 3G⇒WLAN threshold, MIP signaling is sent to complete the layer 3 handover. The use of this model leads to higher MIH signaling load upon cell detection, but avoids possible delay for signaling completion between layer two link detection and the layer three handover processes. A deeper study about this decision can be found in [91].

PoS Design

The PoS is a network entity whose MIHF is registered to the MN's own MIHF, receiving subscribed events. Through the received messages, the PoS tracks down the terminal's position and the quality of its received signal strength. Then, the PoS can supply a remote command for handover initiation depending on the load value in that AP. The PoS intelligence depicted in figure 6.11. This is implemented as a network node with a full 802.21 MIHF stack, having the ability to send and receive MIH signaling encapsulated in UDP packets, and a decision engine for handover execution.
Figure 6.11 relates to the input received at the PoS from the MIHF residing at that network entity, and the verification if a handover is feasible. It is possible to verify that the PoS reacts to three different inputs:

1. reception of a MIH_LINK_PARAMETERS_REPORT from the mobile node.
2. load decreased in a AP.
3. load increased in a AP.

Regarding the reception of a MIH_LINK_PARAMETERS_REPORT, the PoS is confronted with an indication that a mobile node has detected a network point of access and its signal quality is good enough for handover. In case the handover target technology is WLAN, it will verify the load value for the access point whose MAC address is included in the MIH_LINK_PARAMETERS_REPORT message. If it verifies that the load value is below a pre-defined threshold, it will initiate the handover signaling. If an AP's load decreases, the PoS obtains an indication from an access point, that the load value has decreased. The intelligence in PoS begins by evaluating if the load has decreased below a pre-defined threshold, verifying the load change has been high enough to admit more mobile nodes to be attached. If that evaluates to true, the PoS will then verify if it has recently received an indication from a mobile node indicating that it would like to handover to that newly available access point. In case the PoS has not received indication that the mobile node has left the cell range, it will trigger a handover procedure. The rationale for this is as follows: if a mobile node attempts to handover to an access point with too much load, a handover will not occur, and the mobile node will remain attached to the 3G leg, but within range of a WLAN cell. If the MN is still within range, and the PoS detects that the load value is now favorable, since WLAN is preferred to 3G, it will try to initiate an according handover. If an AP's load increases, it is the opposite action: the PoS detects that the load, where the mobile node is currently attached, has increased beyond a pre-defined threshold. With that, it will initiate a handover procedure for that node towards the 3G leg, since 3G is proffered to a congested WLAN.

6.3.6 Results Evaluation

We first present the Mobile Initiated and Network Controlled scenario where no admission control mechanism is applied. Figure 6.12 depicts the percentage of failed handovers. Three speeds have been considered namely, 2, 5 and 10 m/s targeting indoor scenarios. From the graph we can see that by varying the threshold 3G⇒WLAN from -75 up to -65 dBm the percentage of failed handovers as defined above increases to almost 65% in case of 10 m/s. The curves follow a similar shape for 2 and 5 m/s. As can be noted, the

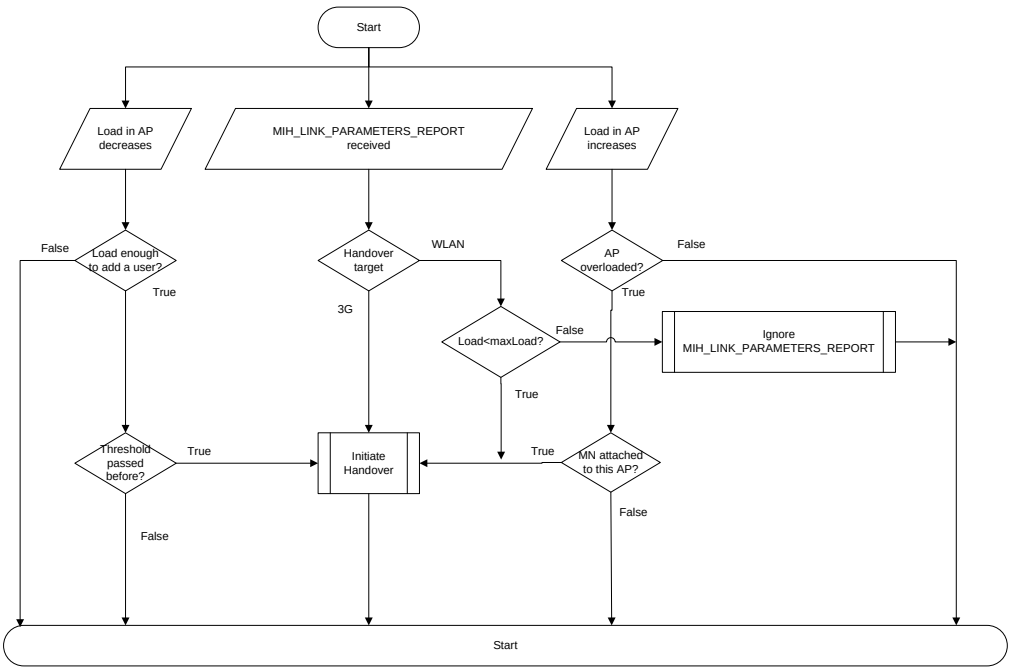


Figure 6.11: PoS Intelligence

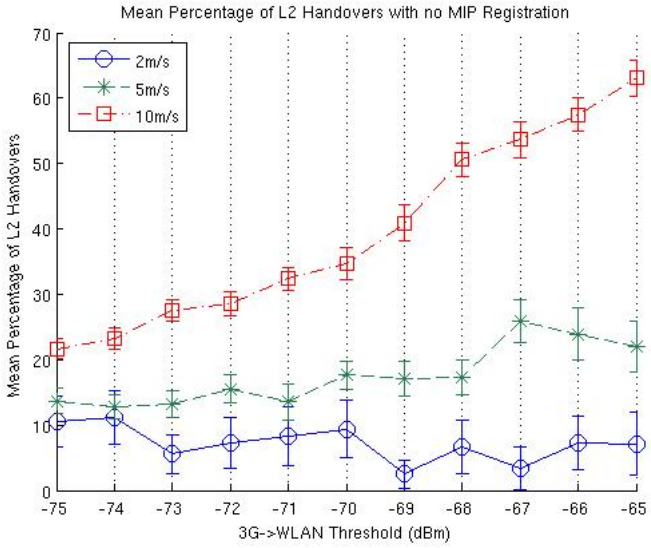


Figure 6.12: Mean percentage of layer two associations not followed by a layer three handover when WLAN⇒3G thresholds configured at -75 dBm

curves show a trend to increase while the 3G⇒WLAN threshold value is increased.

When the mobile node detects the WLAN cell starts the signaling procedure of figure 6.9. After receiving message 6, the mobile node checks the signal level received from the WLAN AP and waits for this level to be over the 3G⇒WLAN threshold for continuing

Speed \ Threshold	-75dBm	-72dBm	-69dBm
Time from sending message 2 to receiving message 6 (3G⇒WLAN)			
2m/s	0.43±0.0002	0.43±0.0002	0.43±0.0002
5m/s	0.422±4.5x10^{-5}	0.422±4.8x10^{-5}	0.422±9.8x10^{-5}
10m/s	0.421±2.8x10^{-5}	0.421±2.8x10^{-5}	0.421±3.03x10^{-5}
Time from sending message 2 to finishing step 7 3G⇒WLAN)			
2m/s	13.6±0.4	20.6±0.8	25.5±1.3
5m/s	4.4±0.07	6.1±0.1	7.6±0.2
10m/s	2.1±0.03	2.9±0.05	3.7±0.07

Speed \ Threshold	-66dBm	-65dBm
Time from sending message 2 to receiving message 6 (3G⇒WLAN)		
2m/s	0.43±0.0005	0.43±0.0002
5m/s	0.422±5.5x10^{-5}	0.422±4.1x10^{-5}
10m/s	0.421±3.4x10^{-5}	0.421±3.3x10^{-5}
Time from sending message 2 to finishing step 7 3G⇒WLAN)		
2m/s	27.1±1.5	28.9±2.2
5m/s	8.5±0.2	9.0±0.3
10m/s	4.1±0.1x10^{-5}	4.3±0.08

Table 6.5: Time required in performing signaling depicted in figure 6.9 for selected 3G⇒WLAN thresholds.

with the signaling. If the signal level never reaches a value over the 3G⇒WLAN threshold, we have a failed handover. This can happen naturally because of the mobility pattern. The mobile approaches the WLAN cell, but because its movement direction, it never reaches the position in the cell where the signal level is above the threshold. Of course, as the 3G⇒WLAN threshold is higher, this happens more often, as can be observed in figure 6.12. Faster speeds also increase the number of failed handovers, because in more occasions the mobile is not enough time in the zone inside the threshold.

An important point for us is the impact of the delay introduced by our required signaling in this procedure. Without the signaling to enable network control (figure 6.9), the mobile node is ready to perform the handover immediately after detecting the WLAN cell. With the signaling, we introduce a delay (the time between message 2 in figure 6.9 and receiving message 6) in which, even if the signal level crosses the threshold, the mobile node cannot perform the handover because it has to wait to complete the signaling with the network. If the delay introduced by the signaling is larger than the time needed to cross the 3G⇒WLAN threshold, the handover is delayed or in the worst case could never happen. We explore this issue in table 6.5 in which the delay from sending message 2 to receiving message 6, and from sending message 2 to finishing step 7, is compared for different speeds and 3G⇒WLAN thresholds. The signaling delay is much lower than the time needed to cross the threshold and completing step 7, showing that the signaling does not interfere with the handover performance. So we argue that the mobile node to network communication is suitable both from a signaling overhead point of view (table 6.3) and from handover performance point of view (table 6.5).

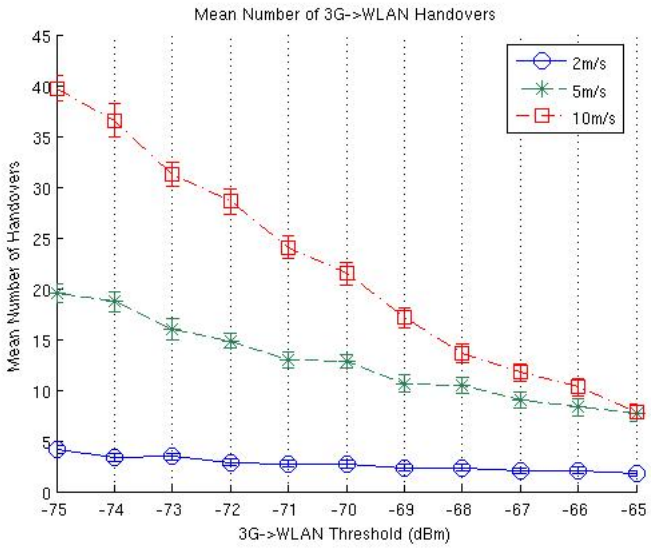


Figure 6.13: Mean number of 3G⇒WLAN handovers when the WLAN⇒3G threshold is configured at -75dBm

Figure 6.13 depicts the mean number of layer three handovers obtained by varying the 3G⇒WLAN threshold. The impact of the speed affects the metric in different ways depending on the considered configuration. At the value -75 dBm the number of handovers is quite large especially considering high mobility level, while decreases and converges for greater values of the threshold. The decay in the slope of the different speeds is related with the failures of performing the layer three handover shown in figure 6.12. The graph shows how the values tend to converge, when the 3G⇒WLAN threshold is increased. The graph presenting the number of handovers from WLAN to 3G is symmetric due to the scenario symmetry. It is interesting to note that the closer the mobile node to the access point, the lower the chance of having complete handovers. This is complementary to the previous graph, as the metric is mostly affected by the mobility pattern and not from the signaling required for mobile to network communication.

Figure 6.14 shows the mean wireless utilization time according to the three different speeds. The general observed behavior is a flat response with the increase of the 3G⇒WLAN threshold. As the primary goal of this study is the maximization of the wireless utilization time, and thus to reduce the number of handovers which do not result in a long term stay inside the cell, figure 6.14 demonstrates that the signaling does not impact the mean wireless utilization metric. In fact, the relative magnitude between the different lines shows that the metric is mostly impacted by the time the user resides in the wireless cell, which result in a higher utilization time at lower terminal speed. This conclusion further supports the explanation of figure 6.12 where the mobility pattern represent the dominant effect on the system.
The results above presented demonstrated that with the values of measurements in table 6.5 the cost of mobile to network signaling for network controlled and initiated handovers is negligible.

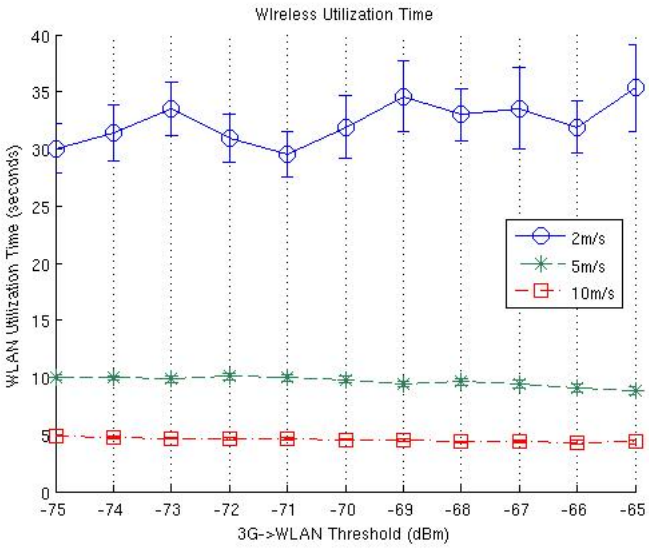


Figure 6.14: Mean wireless utilization time (units of time per handover)

6.4 Conclusions

In this chapter we have presented an exhaustive analysis of the challenges and possibilities of network controlled handovers and their combination with more traditional types of mobility. Starting from current trends both in the research community and standardization bodies, we derive motivations and scenarios where network controlled handovers apply. Through an extensive simulation study we present insightful results on the advantage of applying such technology in future all IP networks. Furthermore, insights on configuration setups that allow operators to maximize the benefit from NIHO techniques are given. We also presented a framework that integrates 802.21 and Mobile IP for Network Controlled Handover support in heterogeneous networking. This framework is evaluated in the usual situation of mixed 3G and WLAN environments. Our results address handover management, heterogeneous networking signaling and decisions making procedures implemented in the network diverging from more classic host based solutions. The results show that the 802.21 usage does not impose significant network load, and that the network handover initiation features provide improved mobility behavior and network utilization. We argue future mobile operators, aiming at the delivery of end to end seamless services across heterogeneous wireless/wired access technologies, will benefit from the analysis of this framework. It should be noted that the study focuses on the conceptual analysis of Network Controlled Handovers in IP environments abstracting from technology specific radio resource management mechanisms.

Part V

Failure Recovery

Chapter 7

Failure Detection and Path Exploration Protocol

7.1 Introduction

This thesis presents an architecture (see chapter 4) which enables mobility and multihoming in future mobile terminals. Chapters 5 and 6 were devoted to present the building blocks used to provide mobility capabilities to the terminal. In this chapter we study the final block, related to failure detection in multihomed and mobile environments.

A fault tolerance solution requires a mechanism to timely detect failures across the communicating path, and a mechanism to discover a valid path after a failure. SHIM6 includes a component, named REAP (REAchability Protocol, [39]), to detect failures in any of the two unidirectional paths in use for a communication, and to explore different unidirectional paths to find a valid one after an outage. Note that REAP understands a bidirectional path as two unidirectional paths.

The REAP instance of an endpoint for a given communication detects a failure if no packets were received for a given period of time. When a communication involves a bidirectional exchange of data at a sufficient rate, the determination of the availability of the path is performed without REAP-specific signaling. If only one of the parties is sending data regularly or the rate at which data is sent is too low, the REAP entities generate Keepalive messages to prevent the expiration of a timer at the other communicating node in the absence of failures. When no party sends upper layer data for some time REAP stops generating Keepalive messages and failure monitoring is no longer being performed. When a failure is detected, REAP triggers the path exploration component. The paths currently in use are first tested by sending REAP Probe messages. If this validation fails, different combinations of source/destination addresses are checked until a new pair of working addresses is found. Note that SHIM6 and REAP support the use of paths defined by different source and destination address pairs on each direction. For more information regarding the operation of REAP please refer to section 3.2.3

A failure detection mechanism should require low resources to operate, and should

waste little bandwidth for signaling purposes. The amount of state required for REAP operation, is three timers per communication and per endpoint. Additionally, it is quite efficient in terms of the number of protocol-specific messages exchanged since Keepalive messages are only sent for unidirectional communications or when the sending rate of data packets is too low. The low requirements exhibited by REAP make this protocol a good candidate for becoming the failure detection and path exploration mechanism of choice for other protocols requiring such functionality, such as HIP [43] or Mobile IPv6 with registration of multiple CoAs [29]. Note that the failure detection component could be independently used for protocols requiring just this functionality. In this section we focus in the study of the REAP protocol assuming that some other protocol is used to manage the paths in use in the data plane, such as SHIM6 or Mobile IPv6 with multiple registrations. A combination of both is proposed in chapter 4.

However, despite the functional simplicity of the REAP mechanism, the characterization of its performance is far from trivial. Although simulation and experimental studies are starting to be performed [82], no analytical characterization of the time required to recover from a failure has been provided so far. Note that this value is a key figure of merit for determining the impact perceived by upper layers. Too large recovery times can result in the communication being discarded by the upper layers. But even if the communication continues, the quality (as defined for each application) can be negatively affected if recovery takes longer than a communication specific threshold. The aim here is not to make failures completely transparent to upper layers, but to make the interruption short enough from the upper layers point of view to not completely disrupt the communication. Proper characterization of REAP performance would enable the configuration in a per-communication basis of the REAP timers in order to comply with specific upper layer constraints.

In this chapter we characterize analytically the upper bound of the time required by REAP to detect a failure and recover from it in different scenarios. We also present insights of the behavior of TCP applications when used with the REAP protocol.

The reminder of this chapter is organized as follows: sections 7.2 to 7.5 are devoted to the analytical study of the time required by REAP to recover the communication after a failure. The final output of these sections is an upper bound of this time for bidirectional and unidirectional traffic regardless of the type and location of the failure. Section 7.6 analyzes by simulation the interaction of TCP mechanisms and REAP, and the effect on recovery of TCP applications. Finally section 7.7 concludes this work.

7.2 Model for performance evaluation in REAP

In this section we present the reference model to be used in the performance analysis for REAP. We first discuss the parameters involved in the failure detection and recovery procedures. Then, we define the figure of merit through which we evaluate the performance of REAP, the Recovery Time.

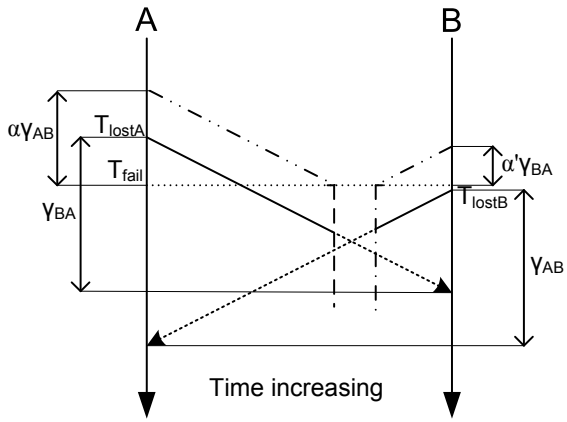


Figure 7.1: Reference Model for the analysis of REAP

7.2.1 Reference Model for REAP

Consider two nodes that are communicating. Packets traveling from A to B, and from B to A, experiment a fixed propagation delay of γ_{AB} and γ_{BA}, respectively which may change when the addresses in use change. Note that γ_{AB} and γ_{BA} can be quite different for many reasons. To name a few, they can be different because, for example, SHIM6 or Mobile IPv6 with multiple registrations allow each direction to be determined by unrelated source and destination addresses, resulting in completely different unidirectional paths, or because even if the same routers were traversed in both directions, queuing delay can be different as a result of different traffics being served for each segment on each direction. The Round Trip Time at a given time is computed as $R_{TT} = \gamma_{AB} + \gamma_{BA}$. Upper layers periodically deliver data packets to the IPv6 layer. Communication can be bidirectional, on this case we suppose node A is sending data with a fixed inter-packet rate of Δ_A, and node B is sending data with Δ_B interval. A communication can be unidirectional, in which case we assume that it is node A the one that sends traffic at a rate Δ_A. The case in which no packets are sent by neither of the peers is not considered, since then, REAP does not perform failure detection. For the rest of the definition of the model we assume bidirectional traffic without loss of generality.
Note that the size of each packet is irrelevant for the analysis.
A failure occurs at a given time T_{fail}. The failure could affect both directions if it is caused by a failure in an element (router or link) shared by both paths, or it can just affect to one direction (either affecting the path from A to B, or from B to A). To precisely characterize the location of the failure so that we can determine which packets were able to pass before the failure and which packets were affected by it, we use α and α' to define the fraction of the propagation delay that a packet should experiment until it reaches the point at which the failure has occurred. Considering a bidirectional failure, a packet sent by A would spend $\alpha * \gamma_{AB}$ until it reaches the failure point, and a packet sent from B would spend $\alpha' * \gamma_{BA}$ until it arrives to the outage (see figure 7.1). Then, we can also state that packets sent from peer A at a time $T = T_{fail} - \alpha\gamma_{AB}$ or later are dropped, as well as packets sent from B later than $T = T_{fail} - \alpha'\gamma_{BA}$. Note that α and α' are unrelated because of the different properties of the communication paths in both directions. However, it is unfeasible to have both α and

α' be equal to 0 or equal to 1.
The time at which the first lost packet from A is sent is named T_{lostA}. The time at which the first lost packet from B is sent is denoted as T_{lostB}. Taking into account that each packet must be the first packet lost at its node, the possible range of values for T_{lostA} and T_{lostB} are presented in equations (7.1) and (7.2).

$$T_{fail} - \alpha\gamma_{AB} \leq T_{lostA} < T_{fail} - \alpha\gamma_{AB} + \Delta_A \quad (7.1)$$

$$T_{fail} - \alpha'\gamma_{BA} \leq T_{lostB} < T_{fail} - \alpha'\gamma_{BA} + \Delta_B \quad (7.2)$$

We do not consider the loss of individual packets or bursts due to transient events such as congestion, so only some transitions of the state machine of REAP are going to be taken into account. We also do not consider new failures occurring during the path exploration process. The impact of this assumptions on the state machine of REAP is discussed on section 7.3.
Finally, we assume that the Send and Keepalive Timers of A and B are equal, with values T_{Send} and T_{KA} respectively.

7.2.2 Recovery Time

The analysis presented in this work aims to characterize the behavior of REAP when an outage occurs. For this purpose, we define the *Recovery Time* as the difference between the time at which the first data packet lost (at any node) is sent, and the time at which every peer willing to send traffic is ready to send packets again (i.e. the peer or peers with traffic to send have returned to the Operational state). In particular, for unidirectional traffic only the peer sending traffic has to return to the Operational state to restore the original communication.
Figure 7.2 shows the Recovery Time for a bidirectional data exchange with a failure affecting both directions. For the sake of clarity, data packet exchanges during the exploration process have been omitted, although they are being sent by both nodes. In the situation depicted, the Send Timer at B expires before the Send Timer at A, so it is B the node that starts probing the current path from B to A. Before any Probe Exploring arrives to A, the Send Timer at A expires, so that it also starts testing the current path from A to B. A Retransmission Timer time after the first Probe was sent, B realizes that the current path is not valid, and starts probing alternative addresses. The first alternative path tested succeeds, so A receives the Probe Exploring message, and issues a Probe Inbound_OK that includes information confirming the validity of the new path from B to A. Upon the successful reception of this message at B, B changes its state to Operational and data packets can be sent again. Finally, a Probe Operational from B to A is used to inform A that the path it had selected is valid. In the example considered, the Recovery Time is the time since the first packet sent by A was lost, until both peers return to Operational state.
As discussed before, the operation of some upper layers may be negatively affected by outages lasting for more than a given threshold, threshold that may vary for different transport and application layer combinations. Consequently, we are particularly interested in being able to estimate the upper bounds for the Recovery Time in any particular scenario determined by the type of communication (bidirectional, unidirectional), the frequency at which data packets are sent in both communicating peers, the Send Timer and Keepalive Timer values, and the propagation times at both directions of the communication. Provided that the parameters characterizing the communication were known, it could be determined if a given

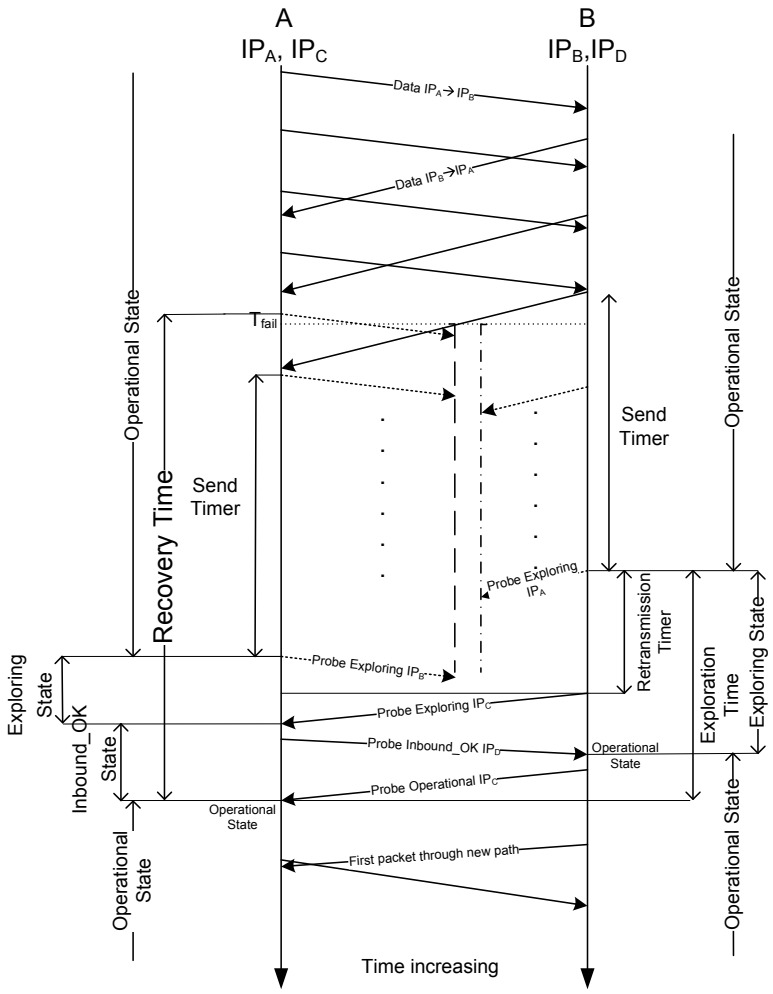


Figure 7.2: Recovery Time Components

configuration fulfills the requirements of the upper layers regardless the particular execution details, such as the exact time at which packets are sent at each side or the failure details, i.e. regardless failure affecting one or both directions or the physical location at which the failure occurs.

7.3 Characterization of the Recovery Time

In order to characterize the behavior of $T_{recovery}$, we have to consider all possible communication scenarios that may result from the type of communication and the scope of the failure:

- Bidirectional traffic, Two-Ways failure.
- Bidirectional traffic, One-Way failure.
- Unidirectional traffic, Two-Ways failure.

- Unidirectional traffic, One-Way failure on data path.
- Unidirectional Traffic, One-Way failure on Keepalive path. Although this scenario is possible, it is not relevant for our work since this kind of failure does not affect the application data exchange.

On the following sub-sections an analysis of the $T_{recovery}$ for each of the cases presented above is performed. During this analysis the following assumptions have been done to simplify the analysis:

- We focus our analysis in path failure cases, therefore the loss of individual packets or bursts due to transient events such as congestion is not modeled.
- The first path explored after a failure is valid. A scenario in which this typically occurs is when the failure affects a single element, and the addresses tested for the candidate paths are disjoint from the addresses previously in use. The supposition is also valid for a concurrent search in which all paths are tested and a valid one exists. We also suppose that a Send Timer period is sufficient for sending a Probe Inbound_OK and receiving its corresponding Probe Operational.

These assumptions reduce the complexity of the state machine of REAP (figure 3.5 presented on section 3.2.3), by deleting some transitions:

- After a failure, a node in Exploring state never receives data packets (that use the original path). Data packets could only be received if the node entered in the Exploring state due to a transient loss of packets.
- Keepalives are only sent in the Operational state. If packets are not lost unless a failure occur, a node is in Exploring state only if the original incoming path failed. Then, Keepalives should not be received through the original incoming path (because it is not available), nor through other path (because a Probe Inbound_OK should have been received before the Keepalive).
- Similarly, Keepalives should not be received in Inbound_OK state because Probe Inbound_OK or Probe Operational messages should have been received before.
- A node can only send Probe Operational messages if it is in the Inbound_OK state and has received a Probe Inbound_OK message. A peer can only send Inbound_OK messages from the Inbound_OK state. Therefore, a node in the Exploring state cannot receive a Probe Operational message.
- As the first explored path after a failure is valid and the Send Timer is large enough, it should not expire in the Inbound_OK state.

Taking these assumptions into consideration and removing the states not related with the exploration from the original state machine of REAP, figure 7.3 presents the simplified state machine of REAP. We use this state machine to derivate on the following sub-sections the feasible transitions for each of the scenarios presented above. It is worth to note that when a failure occurs, the sequence of the first two events is limited to the following: the first event

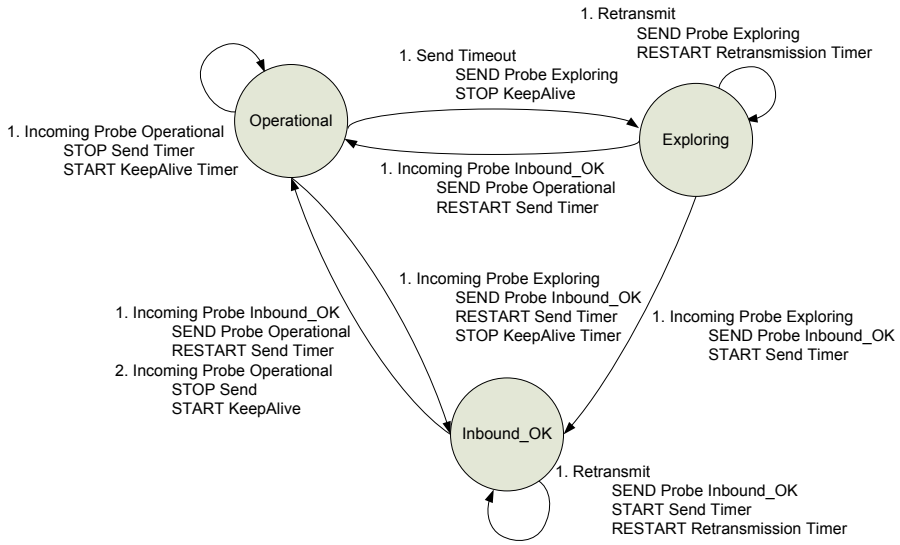


Figure 7.3: REAP Simplified State Machine

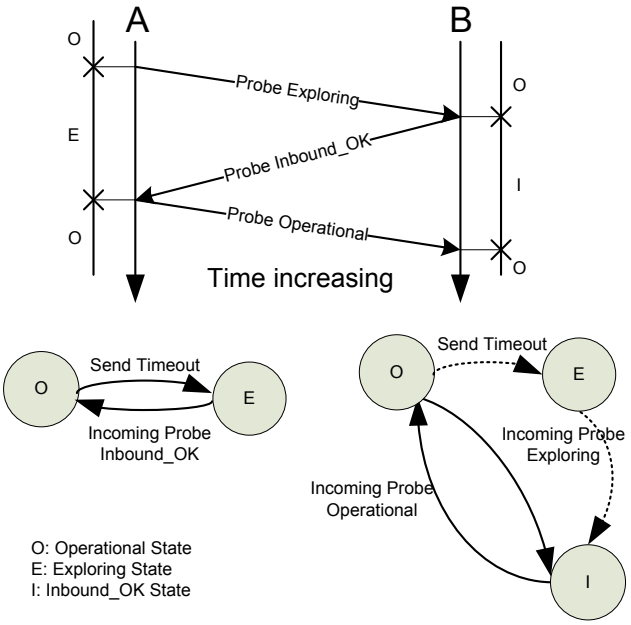
is always the expiration of the Send Timer in any of the nodes, triggering the generation of a Probe Exploring message. Then, only two possibilities are available for the transitions on the peer node: the peer remains in Operational state until receiving the Probe Exploring message, or, only for bidirectional communication with two-ways failure, the Send Timer could expire before receiving the Probe Exploring message. For analyzing the rest of the possible state transitions, we consider the type of traffic and the type of failure.

7.3.1 Bidirectional traffic, Two-Ways failure

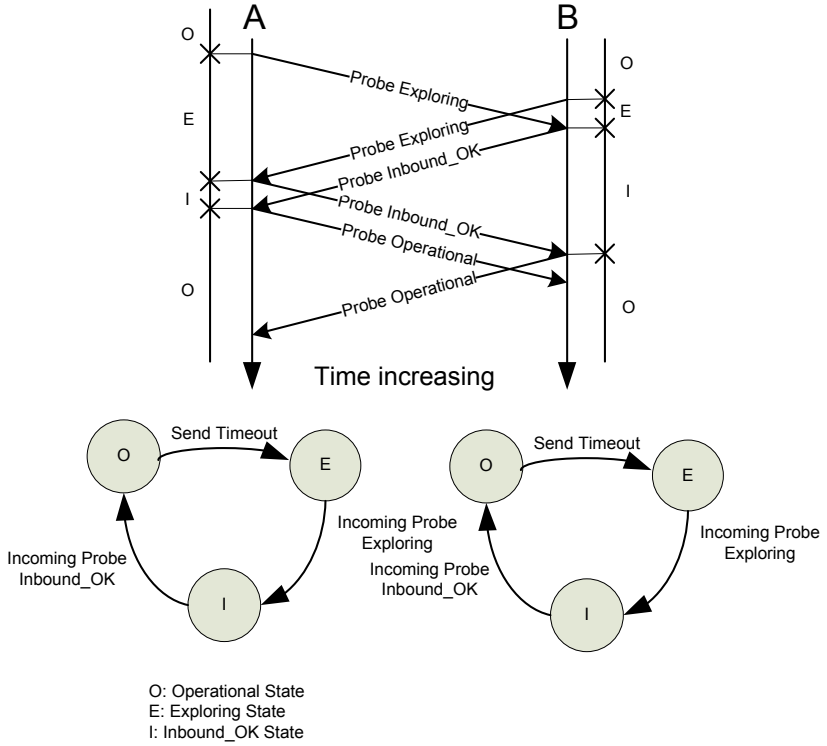
On this scenario, the peers are exchanging bidirectional traffic when both unidirectional paths in use are affected by an outage. The restriction that a node can only reach the Inbound_OK state when the peer is in the Exploring state defines three possible state sequences in the peers until they return to the Operational state (Figure 7.4).
In the first case, presented on figure 7.4(a) (continuous lines), the node discovering the failure after the expiration of the Retransmission Timer, A, sends a second Probe Exploring message that arrives to its peer B when it is in Operational state. The reception of the Probe Exploring results in a change to Inbound_OK in B. On this transition, B sends a Probe Inbound_OK message, which after reception triggers a transition in A from the Exploring state to the Operational. Hence, the peer which transits to Operational state sends a Probe Operational message to alter the state of the corresponding peer to Operational state. At this point both peers are ready to resume the communication. Taking into account this behavior, equation (7.3) presents the value of $T_{recovery}$ for this scenario.

$$T_{recovery} = T_{RTx} + R_{TT} + \gamma + T_{send} + min(\tau_A, \tau_B) \tag{7.3}$$

We define τ_A (τ_B) as the time elapsed between the sending of the first packet lost (in any node) and the starting time of the Send Timer on A (B). In the case considered, we are interested the time at which the first node detecting the failure starts its Send Timer (in



(a) Probe Exploring sent by A arrives at B before B enters into Exploration State.



(b) Both peers are in Exploring State when a valid path is discovered

Figure 7.4: Path Exploration Transitions: Bidirectional traffic, Two-Ways failure

Figure 7.4(a), node A), condition that is expressed in general as $min(\tau_A, \tau_B)$. Then after T_{send} time, node A sends a Probe Exploring that is never returned, so the Retransmission Timer expires after T_{RTx} seconds. A new path is explored by sending a Probe Exploring message, requiring $\gamma_{AB} + \gamma_{BA} + \gamma_{AB}$, or in other words, $R_{TT} + \gamma$, being γ the propagation time from the node discovering the failure to its peer.
The second case corresponds to figure 7.4(a) (dashed lines). On this case, node A reaches the Exploring state before node B. The first Probe Exploring message sent by B is lost since this message is sent through the failed path. While node B is in the Exploring state, node A sends a Probe Exploring message that reaches node B, changing its state to Inbound_OK. On this transition, node B sends a Probe Inbound_OK message. When this message reaches node A it changes its state to Operational, sending a Probe Operational message, which after reception, changes the state of node B to Operational. At this point both peers are ready to resume the communication. This state sequence yields to the same equation as the first case (equation (7.3)).
The third case corresponds to figure 7.4(b). On this case, peer B reaches the Exploring state prior to receiving the Probe Exploring message from A. On this scenario both peers perform the transition Exploring→Inbound_OK→Operational and are able to resume the communication once a Probe Inbound_OK is received (Equation (7.4)).

$$T_{recovery} = T_{RTx} + R_{TT} + T_{send} + max(\tau_A, \tau_B) \tag{7.4}$$

Now, the time at which the process is finished is driven by the node that detected the failure last.

7.3.2 Bidirectional traffic, One-Way failure

Figure 7.5 presents the only possible state sequence for path exploration on a scenario where bidirectional traffic is affected by an outage on the unidirectional path (in this case, from A to B). As the Send Timer is set each time a packet is sent and stopped each time a packet is received, the Send Timer on peer A never expires since the path from B to A is not affected by the outage. On the other hand, due to the outage, B does not receive packets from A so its Send Timer expires triggering a transition to the Exploring State. Then B sends a Probe Exploring message, which is received by A, transits to the Inbound_OK state. This Probe Exploring message reaches A using the current path, since the path from B to A is not affected by the outage. On this transition, A sends a Probe Inbound_OK to B, using the current path, that it is lost. A new Probe Inbound_OK message sent through other paths succeeds in arriving to B. As a consequence, B moves to the Operational state again, sending an Operational Probe to A. Once received the Probe Operational, A transits to Operational. Equation (7.5) presents the value of $T_{recovery}$ for this scenario.

$$T_{recovery} = T_{RTx} + R_{TT} + \gamma_{BA} + T_{send} + \tau_B \tag{7.5}$$

Note that the state transition sequences presented above is the only possible one, since the Send Timer can expire only in one of the nodes.

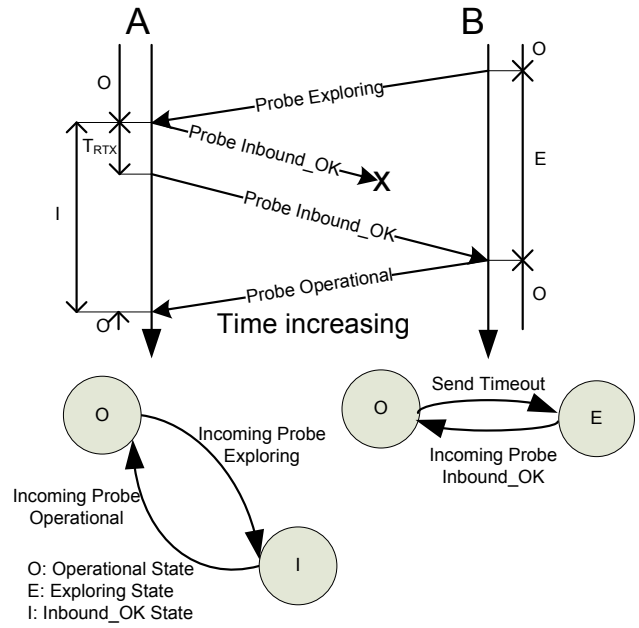


Figure 7.5: Path Exploration Transitions: Bidirectional traffic, One-Way failure

7.3.3 Generic case for Bidirectional Traffic

Given the equations for $T_{recovery}$ presented on the previous sub-sections, we now provide a general expression to be used for Bidirectional Traffic, regardless the type of failure.

$$T_{recovery} = T_{RTx} + R_{TT} + T_{send} + min(\tau + \gamma, \tau_c) \tag{7.6}$$

On equation (7.6), τ corresponds to the peer which Send Timer expires first ($min(\tau_A, \tau_B)$). γ is the propagation time between the node which Send Timer expires first and the peer. τ_c is the τ of the node which Send Timer expires the last ($max(\tau_A, \tau_B)$). The case $\tau + \gamma < \tau_c$ corresponds to the first Probe Exploring message sent through a valid path reaching the peer while it is still on the Operational state. The case $\tau + \gamma > \tau_c$ corresponds to the first Probe Exploring message reaching the peer when it is on the Exploring state. Finally it is worth to note that the Bidirectional traffic, One-Way failure case (equation (7.5)) is just a particular case of expression (7.6) in which $max(\tau_A, \tau_B) = \infty$.

7.3.4 Unidirectional traffic, Two-Ways failure

On this scenario only one possible state sequence is possible. As the Send Timer is set up each time a packet is sent, the Send Timer is only running on the node sending the packets. Figure 7.6 presents the state sequence and the messages exchanged for the path exploration mechanism on this scenario in which node A is the sending active peer. When the failure occurs, A stops receiving Keepalive messages and its Send Timer expires, changing its state to Exploring and sending a Probe Exploring message. Upon reception of the Probe Exploring message, node B modifies its state to Inbound_OK and sends a Probe Inbound_OK message to A. When this probe is received on A, its state changes to Operational and a Probe

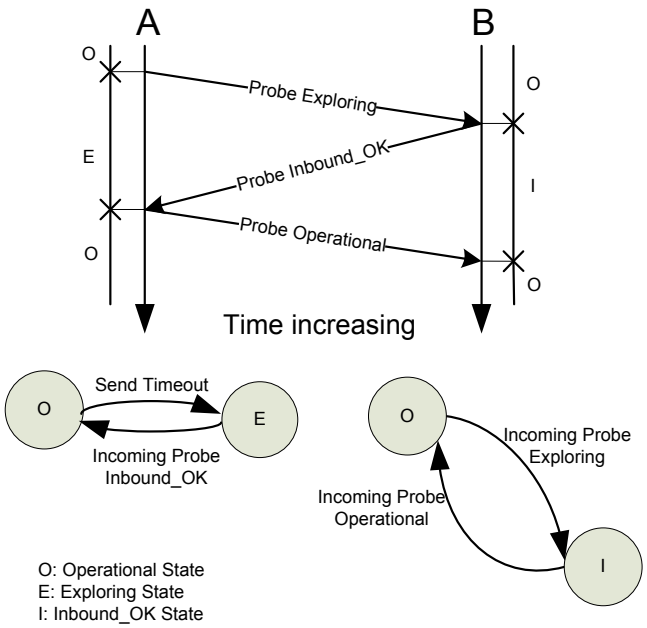


Figure 7.6: Path Exploration Transitions: Unidirectional Traffic, Two-Ways failure

Operational message is sent to B. Once A reaches the Operational state again the application is ready to resume the communication. Equation (7.7) presents the value of $T_{recovery}$ for this scenario.

$$T_{recovery} = T_{RTx} + R_{TT} + T_{send} + \tau_A \tag{7.7}$$

7.3.5 Unidirectional Traffic, One-Way failure on the data path

Due to the characteristics of REAP, this scenario corresponds exactly to the same state machine transitions as on the previous sub-section. Note that the $T_{recovery}$ value on this case is different from the previous section, being τ the difference between both cases.

7.4 Characterization of τ

Most of the components of the expressions presented in section 7.3 are simple to characterize. However, that is not the case for the τ parameter. On the following sections we provide a set of equations to characterize τ for each of the cases presented on section 7.3. The results are upper bounds of τ that are always a *supremum* (or least upper bound, i.e. the smallest real number that is greater than or equal to every possible τ). We use the term *maximal* for the case in which there is a τ that equals to the *upper bound*, leaving the term supremum for the case in which τ never reaches the upper bound.

7.4.1 Bidirectional traffic, Two-Ways failure

The approach followed for characterizing τ is to identify the only four cases in which the maximum value for τ can occur regardless the starting times for sending packets at A

and B and the time of the failure:

- Case π: The first packet lost was sent by A, and τ_A reaches its maximum value ($\tau_{A\pi}$).
- Case θ: The first packet lost was sent by B, and τ_B reaches its maximum value ($\tau_{B\theta}$).
- Case ρ: The first packet lost was sent by A, and τ_B reaches its maximum value ($\tau_{B\rho}$).
- Case σ: The first packet lost was sent by B, and τ_A reaches its maximum value ($\tau_{A\sigma}$).

Taking into account the values of τ_A and τ_B for each of the scenarios described above, the maximum value of τ is:

$$\tau_{max} = max\Big[min(\tau_{A\pi}, \tau_{B\pi}), min(\tau_{B\theta}, \tau_{A\theta}), min(\tau_{B\rho}, \tau_{A\rho}), min(\tau_{A\sigma}, \tau_{B\sigma})\Big] \quad (7.8)$$

On the following sub-sections we continue the characterization of the Bidirectional traffic, Two-Ways failure by obtaining the values for each of these situations. Then we prove that it is impossible to find a case, μ, in which $min(\tau_{A\mu}, \tau_{B\mu}) > \tau_{max}$, demonstrating that the maximum must occur in any of the four cases identified. A more general expression, independent from the specific location of the point of failure, of an upper bound of τ (τ_{upp}) is provided on section 7.5.
Please note that although on this section we focus on finding the τ which first triggers the exploring mechanism on the first node detecting the failure, the τ corresponding to the peer is also calculated. Once τ_{max} is found, it is easy to obtain the expression for τ on the peer node for each of the cases (π, θ, ρ and σ).

Case π

We first identify the case in which the maximum delay between the loss of the first packet sent by A and the start of the Send Timer on A occurs. Then we analyze the values of τ_A and τ_B for this specific scenario.
The worst case scenario on this situation (figure 7.7), that depends on the timing of the packets sent at both nodes, corresponds to the exchange of packets which leads to the greatest difference between T_{recA} (time at which the last packet sent by B arrives at A) and T_{lostA} (sending time of the first packet lost on A). This difference is the greatest when T_{lostA} corresponds to the lowest possible value and T_{recA} to its highest value. T_{send} will be started on A when the next packet is sent by A after the last packet from B was received (T_{recA}, see Figure 7.7). Considering that A sends a new packet each Δ_A seconds, the value of $\tau_{A\pi}$ can be expressed using the ceil function as $\lceil \frac{T_{recA} - T_{lostA}}{\Delta_A} \rceil \Delta_A$.
In order for T_{recA} to be the highest value, the last packet which arrived correctly to peer A must be sent at the latest possible time, hence T_{lostB} approaches to the highest limit imposed on equation (7.2). On the same way, in order for T_{lostA} to be the lowest value, it must reach the lowest limit imposed by equation (7.1). Following the reasoning presented above, equation (7.9) presents the values for T_{lostA}, T_{lostB} and T_{recA}, with $\epsilon \to 0$. To represent the packet at B sent just before the failure could drop the packet.

$$\begin{aligned} T_{lostA} &= T_{fail} - \alpha\gamma_{AB} \\ T_{lostB} &= T_{fail} - \alpha'\gamma_{BA} + \Delta_B - \epsilon \\ T_{recA} &= T_{lostB} + \gamma_{BA} - \Delta_B \end{aligned} \quad (7.9)$$

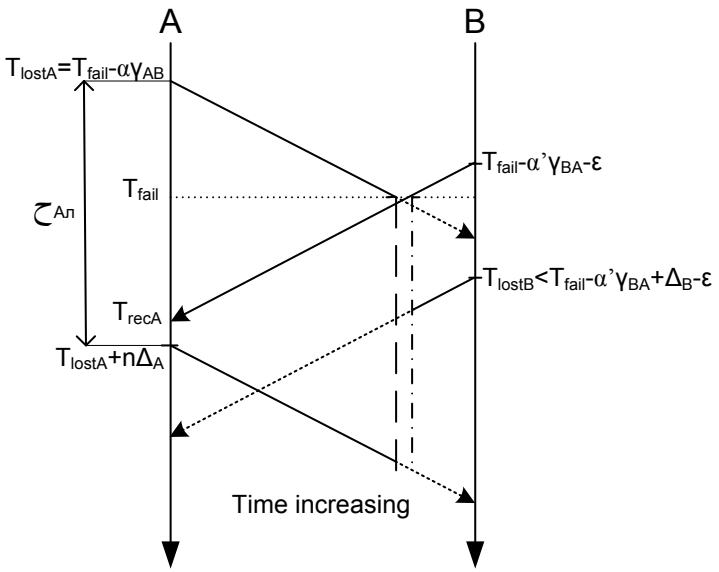


Figure 7.7: Maximum $\tau_{A\pi}$ for first packet lost sent by A

Therefore:

$$T_{recA} - T_{lostA} = (1 - \alpha')\gamma_{BA} + \alpha\gamma_{AB} - \epsilon$$

Note that as ϵ tends to zero, its contribution is irrelevant inside the ceil approximation, hence $\tau_{A\pi}$ is a maximal of τ.

$$\tau_{A\pi} = \left\lceil \frac{(1 - \alpha')\gamma_{BA} + \alpha\gamma_{AB}}{\Delta_A} \right\rceil \Delta_A \tag{7.10}$$

We now characterize the corresponding value of τ on peer B ($\tau_{B\pi}$). The Send Timer on peer B is started on the next packet sent after the reception of the last packet from peer A (T_{recB}, see Figures 7.8 and 7.9). By definition, $\tau_{B\pi}$ is

$$\tau_{B\pi} < T_{sendB} - T_{lostA} \tag{7.11}$$

Depending on the packet timing and the propagation times, two situations could occur: i) $T_{lostB} \leq T_{recB}$ and ii) $T_{lostB} > T_{recB}$.
For $T_{lostB} \leq T_{recB}$ (see figure 7.8), equation (7.12) presents the relation between the propagation times, α, and the packet timing of each node which makes $T_{lostB} < T_{recB}$.

$$\begin{aligned} T_{recB} &= T_{lostA} + \gamma_{AB} - \Delta_A \\ T_{recB} &= T_{fail} + (1 - \alpha)\gamma_{AB} - \Delta_A \\ T_{recB} \geq T_{lostB} &\Rightarrow (1 - \alpha)\gamma_{AB} + \alpha'\gamma_{BA} \geq \Delta_A + \Delta_B \end{aligned} \tag{7.12}$$

Note that the values of T_{lostA} and T_{lostB} are the same of equation (7.9). To calculate the moment at which the Send Timer is set on peer B, we consider two steps. First the distance between T_{recB} and T_{lostB} is calculated. The next packet sent by B after T_{recB} is the packet

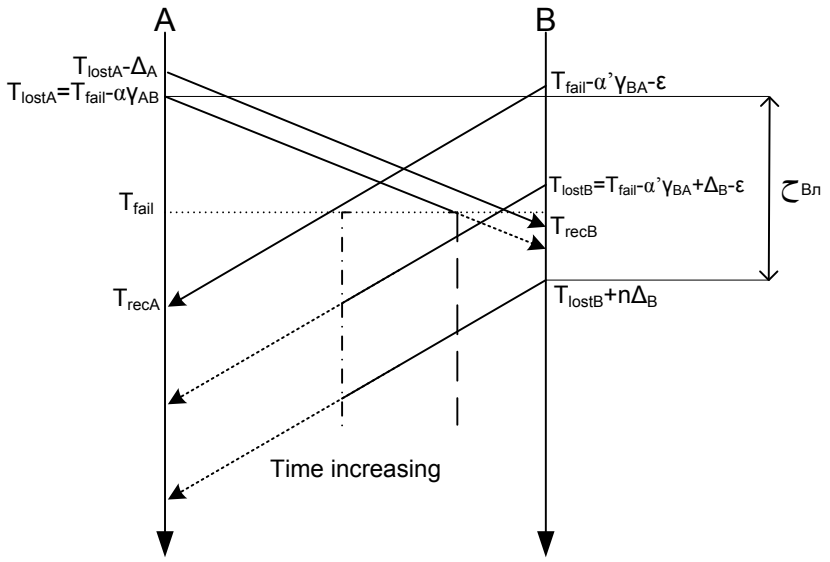


Figure 7.8: Value of $\tau_{B\pi}$ when $T_{lostB} \leq T_{recB}$ for Maximum τ_A and first packet lost sent by A

starting the Send Timer. In this way we know the instant at which the Send Timer is started after T_{lostB}. On the second step, the distance between T_{lostB} and T_{lostA} is calculated. Adding this two values we obtain $\tau_{B\pi}$.

$$\tau_{B\pi} < \left\lceil \frac{T_{recB} - T_{lostB}}{\Delta_B} \right\rceil \Delta_B + (T_{lostB} - T_{lostA}) \tag{7.13}$$

From the T_{recB} expression presented at (7.12), we obtain:

$$\left\lceil \frac{T_{recB} - T_{lostB}}{\Delta_B} \right\rceil \Delta_B = \left\lceil \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} - \Delta_A - \Delta_B}{\Delta_B} \right\rceil \Delta_B \tag{7.14}$$

$T_{lostB} - T_{lostA}$ can be computed as follows.

$$T_{lostB} - T_{lostA} = \alpha\gamma_{AB} + \alpha'\gamma_{BA} + \Delta_B - \epsilon \tag{7.15}$$

Note that $T_{lostB} > T_{lostA}$ since we have defined on the scenario that the first packet lost was sent by A. Combining expressions (7.13), (7.14) and (7.15) on equation (7.16),

$$\tau_{B\pi} = \alpha\gamma_{AB} - \alpha'\gamma_{BA} + \Delta_B + \left\lceil \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} - \Delta_A - \Delta_B}{\Delta_B} \right\rceil \Delta_B \tag{7.16}$$

Now we focus on solving equation (7.11) for the case $T_{lostB} > T_{recB}$ (see figure 7.9). T_{sendB} corresponds to the sending time of the next packet sent by B after receiving the last packet from A (T_{recB}). Equations (7.17) and (7.18) present the value of T_{lostB} and T_{lostA} for this case.

$$T_{lostB} = T_{fail} - \alpha'\gamma_{BA} + \Delta_B - \epsilon \tag{7.17}$$

$$T_{lostA} = T_{fail} - \alpha\gamma_{AB} \tag{7.18}$$

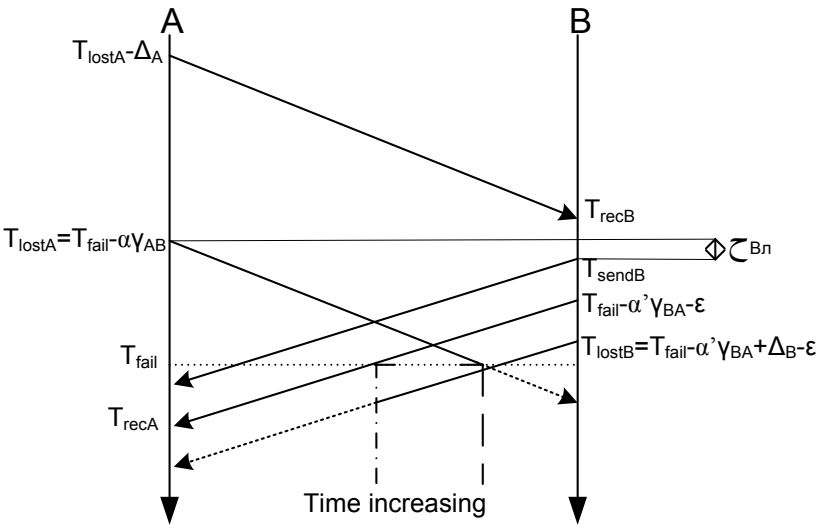


Figure 7.9: Value of $\tau_{B\pi}$ when $T_{lostB} > T_{recB}$ for Maximum τ_A and first packet lost sent by A

The distance between T_{lostB} and T_{recB} can be calculated taking into account the values of equations (7.17) and (7.18).

$$\begin{aligned} T_{recB} &= T_{lostA} + \gamma_{AB} - \Delta_A \\ T_{recB} &= T_{fail} + (1-\alpha)\gamma_{AB} - \Delta_A \\ T_{lostB} - T_{recB} &= -\alpha'\gamma_{BA} - (1-\alpha)\gamma_{AB} + \Delta_A + \Delta_B - \epsilon \end{aligned} \tag{7.19}$$

T_{sendB} can be obtained by considering the number of Δ_B that fit into the distance between T_{lostB} and T_{recB}. The value of T_{sendB} is presented on equation (7.20).

$$T_{sendB} = T_{lostB} - \left\lfloor \frac{-\alpha'\gamma_{BA} - (1-\alpha)\gamma_{AB} + \Delta_A + \Delta_B - \epsilon}{\Delta_B} \right\rfloor \Delta_B \tag{7.20}$$

Combining equations (7.17) and (7.18) the relationship between T_{lostA} and T_{lostB} is

$$T_{lostB} - T_{lostA} = \alpha\gamma_{AB} - \alpha'\gamma_{BA} + \Delta_B - \epsilon \tag{7.21}$$

Including equations (7.20) and (7.21) into equation (7.11), we can find a supremum (due to the influence of the ϵ) to the value of τ_B as shown in equation (7.22).

$$\tau_{B\pi} = \alpha\gamma_{AB} - \alpha'\gamma_{BA} + \Delta_B - \left\lfloor \frac{-\alpha'\gamma_{BA} - (1-\alpha)\gamma_{AB} + \Delta_A + \Delta_B}{\Delta_B} \right\rfloor \Delta_B \tag{7.22}$$

A summary of the values for $\tau_{B\pi}$ is provided next:

- if $(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} \geq \Delta_A + \Delta_B$

$$\tau_{B\pi} = \alpha\gamma_{AB} - \alpha'\gamma_{BA} + \Delta_B + \left\lceil \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} - \Delta_A - \Delta_B}{\Delta_B} \right\rceil \Delta_B$$

- if $(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} < \Delta_A + \Delta_B$

$$\tau_{B\pi} = \alpha\gamma_{AB} - \alpha'\gamma_{BA} + \Delta_B - \left\lfloor \frac{-\alpha'\gamma_{BA} - (1-\alpha)\gamma_{AB} + \Delta_A + \Delta_B}{\Delta_B} \right\rfloor \Delta_B \quad (7.23)$$

being $\tau_{B\pi}$ a supremum of τ. Note that for the second case, $\tau_B < \tau_{B\pi} < \tau_B + \Delta_B$.

Case θ

Due to the symmetry of the system, τ on B when the first packet lost is sent by B corresponds to the same scenario as $\tau_{A\pi}$ swapping node A by node B. The equations defining $\tau_{B\theta}$ can be obtained following the procedure used on section 7.4.1 after exchanging Δ_A by Δ_B, α by α', γ_{AB} by γ_{BA} and γ_{BA} by γ_{AB} on equations (7.9) and (7.10):

$$\tau_{B\theta} = \left\lceil \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA}}{\Delta_B} \right\rceil \Delta_B \quad (7.24)$$

As on the case of $\tau_{A\pi}$, $\tau_{B\theta}$ is a maximal of τ.
Correspondingly, $\tau_{A\theta}$ is symmetric to $\tau_{B\pi}$, so

- if $(1-\alpha')\gamma_{BA} + \alpha\gamma_{AB} \geq \Delta_A + \Delta_B$

$$\tau_{A\theta} = \alpha'\gamma_{BA} - \alpha\gamma_{AB} + \Delta_A + \left\lceil \frac{(1-\alpha')\gamma_{BA} + \alpha\gamma_{AB} - \Delta_A - \Delta_B}{\Delta_A} \right\rceil \Delta_A$$

- if $(1-\alpha')\gamma_{BA} + \alpha\gamma_{AB} < \Delta_A + \Delta_B$

$$\tau_{A\theta} = \alpha'\gamma_{BA} - \alpha\gamma_{AB} + \Delta_A - \left\lfloor \frac{-\alpha\gamma_{AB} - (1-\alpha')\gamma_{BA} + \Delta_A + \Delta_B}{\Delta_A} \right\rfloor \Delta_A \quad (7.25)$$

As on the case of $\tau_{B\pi}$, $\tau_{A\theta}$ is a supremum of τ_A ($\tau_A < \tau_{A\theta} < \tau_A + \Delta_A$).

Case ρ

On this section, we identify the situation in which the maximum delay between the loss of the first packet sent by A and the start of the Send Timer on B occurs. Then we analyze the values of τ_A and τ_B for this specific scenario. Figure 7.10 presents the worst case scenario for setting the Send Timer on B ($\tau_{B\rho}$) when the first lost packet corresponds to A. The time at which B receives the last packet from A (T_{recB}) is stated on equation (7.26).

$$T_{recB} = T_{lostA} + \gamma_{AB} - \Delta_A \quad (7.26)$$

The time when the Send Timer is set on B corresponds to the next packet sent after receiving the last packet from A. Regardless from the sending time of the last packet from A, on the worst possible case, B sends a packet Δ_B seconds after T_{recB}, being this time T_{sendB}. The value of τ for this case, that is a maximal, is presented on equation (7.27).

$$\begin{aligned} \tau_{B\rho} &= T_{sendB} - T_{lostA} = T_{recB} + \Delta_B - T_{lostA} \\ \tau_{B\rho} &= \gamma_{AB} - \Delta_A + \Delta_B. \end{aligned} \quad (7.27)$$

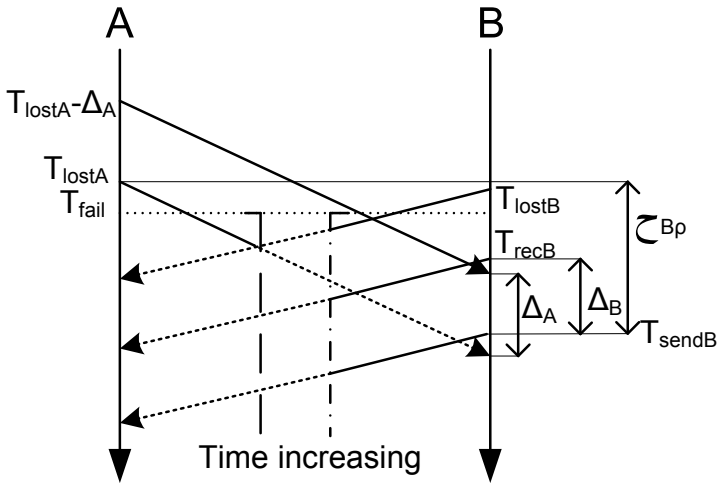


Figure 7.10: Maximum $\tau_{B\rho}$ for first packet lost sent by A

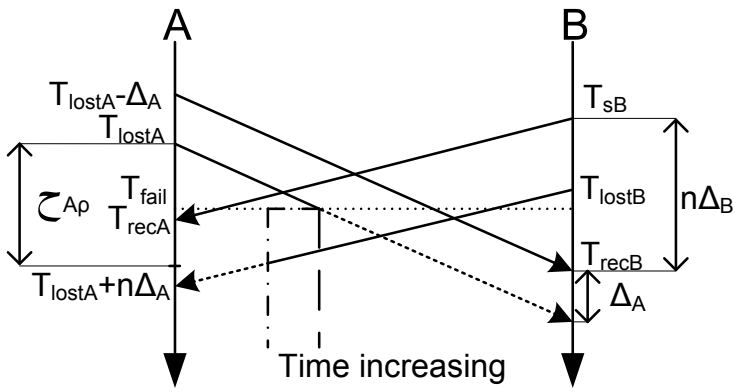


Figure 7.11: Value of $\tau_{A\rho}$ for Maximum τ_B and first packet lost sent by A

Note that the worst possible case of τ_B on this scenario corresponds to the arrival of the last packet sent successfully by A just after B sends a packet.

In figure 7.11 we detail the relevant parameters for this case on node A. The Send Timer on A is started on the next packet sent by A once the last packet sent from B to A arrives (T_{recA}). Therefore,

$$\tau_{A\rho} = \lceil \frac{T_{recA} - T_{lostA}}{\Delta_A} \rceil \Delta_A \tag{7.28}$$

We estimate the time at which the last packet from B arrives (T_{recA}) considering the time at which this packet was sent, T_{sB}, plus the propagation time from B to A.

$$T_{recA} = T_{sB} + \gamma_{BA} \tag{7.29}$$

We can set a relation between T_{sB} and T_{lostA} by analyzing the relationship among the time at which the last packet received at B arrived (T_{recB}) and T_{sB} through a new parameter n.

$$T_{sB} = T_{lostA} + \gamma_{AB} - \Delta_A - n\Delta_B \tag{7.30}$$

Note that we are able to calculate the value of T_{sB} (sending time on B) from a reception time since the scenario explained at the beginning of this sub-section imposes that the sending times on B are immediately before the receiving.
To find the value of n we know that T_{sB} must be the greatest possible value lower than T_{lostB} in order to be received on A ($T_{sB} < T_{fail} - \alpha'\gamma_{BA}$).

$$\begin{aligned} T_{lostA} + \gamma_{AB} - \Delta_A - n\Delta_B &< T_{fail} - \alpha'\gamma_{BA} \\ T_{lostA} &= T_{fail} - \alpha\gamma_{AB} \\ n\Delta_B &> \alpha'\gamma_{BA} + (1-\alpha)\gamma_{AB} - \Delta_A \\ n &= \left\lceil \frac{\alpha'\gamma_{BA} + (1-\alpha)\gamma_{AB} - \Delta_A}{\Delta_B} \right\rceil \end{aligned} \tag{7.31}$$

Equation (7.32) shows the time at which the first packet sent from B is received on A and combines equations (7.28), (7.29), (7.30) and (7.31) to find the final value for $\tau_{A\rho}$.

$$\tau_{A\rho} = \left\lceil \frac{R_{TT} - \Delta_A - \left\lceil \frac{\alpha'\gamma_{BA} + (1-\alpha)\gamma_{AB} - \Delta_A}{\Delta_B} \right\rceil \Delta_B}{\Delta_A} \right\rceil \Delta_A \tag{7.32}$$

being $\tau_{A\rho}$ a maximal of τ.

Case σ

Due to symmetry considerations, $\tau_{A\sigma}$ corresponds to the same scenario as $\tau_{B\rho}$, after swapping node A by node B. The equations can be obtained following the same procedure used on section 7.4.1, i.e. exchanging Δ_A by Δ_B, α by α', γ_{AB} by γ_{BA} and γ_{BA} by γ_{AB} on equation (7.26).

$$\tau_{A\sigma} = \gamma_{BA} - \Delta_B + \Delta_A \tag{7.33}$$

being $\tau_{A\sigma}$ a maximal of τ. The corresponding case on B ($\tau_{B\sigma}$) is

$$\tau_{B\sigma} = \left\lceil \frac{R_{TT} - \Delta_B - \left\lceil \frac{\alpha\gamma_{AB} + (1-\alpha')\gamma_{BA} - \Delta_B}{\Delta_A} \right\rceil \Delta_A}{\Delta_B} \right\rceil \Delta_B$$

being $\tau_{B\sigma}$ is a maximal of τ.

Proof of the Maximality of τ_{max}

On the following lines we prove that equation (7.8) provides a maximum for all possible combinations of τ_A and τ_B, i.e. $\forall \tau_{A\mu}, \tau_{B\mu}. \nexists \tau / \tau = min(\tau_{A\mu}, \tau_{B\mu})$ greater than the τ_{max} given by equation (7.8). Due to the symmetry inherent to equation (7.8) we focus on proving for the case in which the first packet lost is sent by A, that

$$\forall \tau_{A\mu}, \tau_{B\mu} / \tau = min(\tau_{A\mu}, \tau_{B\mu}) \Rightarrow \tau \leq max\Big[min(\tau_{A\pi}, \tau_{B\pi}), min(\tau_{B\rho}, \tau_{A\rho})\Big] \tag{7.34}$$

for every possible case of $\tau_{A\mu}$ and $\tau_{B\mu}$ when the first packet lost is sent by A. An analogous demonstration can be done for the cases when the first packet lost is sent by B.
To prove equation (7.34), we consider the four possible combinations of the values of $\tau_{A\pi}$, $\tau_{B\pi}$, $\tau_{A\rho}$ and $\tau_{B\rho}$:

1. $\tau_{A\pi} < \tau_{B\pi}$ and $\tau_{A\rho} < \tau_{B\rho} \Rightarrow \tau \leq max(\tau_{A\pi}, \tau_{A\rho})$
2. $\tau_{B\pi} < \tau_{A\pi}$ and $\tau_{B\rho} < \tau_{A\rho} \Rightarrow \tau \leq max(\tau_{B\pi}, \tau_{B\rho})$
3. $\tau_{A\pi} < \tau_{B\pi}$ and $\tau_{B\rho} < \tau_{A\rho} \Rightarrow \tau \leq max(\tau_{B\rho}, \tau_{A\pi})$
4. $\tau_{B\pi} < \tau_{A\pi}$ and $\tau_{A\rho} < \tau_{B\rho} \Rightarrow \tau \leq max(\tau_{B\pi}, \tau_{A\rho})$

Note that, as explained on section 7.4.1, by definition $\tau_{A\pi} > \tau_{A\rho}$ and $\tau_{B\rho} > \tau_{B\pi}$, since $\tau_{A\pi}$ and $\tau_{B\rho}$ are the worst possible cases for τ_A and τ_B respectively.
Consider the combination 1. We have to show that $\forall \tau, \tau \leq max(\tau_{A\pi}, \tau_{A\rho})$. As $\tau_{A\pi} > \tau_{A\rho}$ the maximum is $\tau_{A\pi}$, it should be proved that $\forall \tau_{A\mu}, \tau_{B\mu}, \tau = min(\tau_{A\mu}, \tau_{B\mu}) \leq \tau_{A\pi}$. We know that $\forall \tau_{A\mu}, \tau_{A\mu} < \tau_{A\pi}$. For every value of $\tau_{A\mu}$ and $\tau_{B\mu}$, $\tau = min(\tau_{A\mu}, \tau_{B\mu})$ at least is as small as $\tau_{A\mu}$, and this is smaller than $\tau_{A\pi}$, proving that $\tau \leq \tau_{A\pi}$ for all possible combination of $\tau_{A\mu}$ and $\tau_{B\mu}$ with the constrains imposed by the first combination. The same reasoning can be applied to the second case, combination 2, to show that, in this case, $\tau \leq max(\tau_{B\pi}, \tau_{B\rho}) = \tau_{B\rho}$. Focusing on the third case (combination 3). This case imposes $\tau_{B\rho} < \tau_{A\rho}$ and $\tau_{A\pi} < \tau_{B\pi}$, hence $\tau_{A\pi} < \tau_{A\rho}$. Since $\tau_{A\pi} > \tau_{A\rho}$ by definition, this case is not possible.
Finally for the fourth case (combination 4), we have to show that for all combinations of $\tau_{A\mu}$ and $\tau_{B\mu}$, $\tau \leq max(\tau_{B\pi}, \tau_{A\rho})$. $\tau = min(\tau_{A\mu}, \tau_{B\mu})$ so we have to prove that there is not a value of $\tau_{A\mu}$ and $\tau_{B\mu}$ which $min(\tau_{A\mu}, \tau_{B\mu}) > max(\tau_{B\pi}, \tau_{A\rho})$. This is equivalent to prove that the values of $\tau_{A\mu}$ and $\tau_{B\mu}$ are not within the intervals $\tau_{B\pi} < \tau_{B\mu} < \tau_{B\rho}$ and $\tau_{A\rho} < \tau_{A\mu} < \tau_{A\pi}$ at the same time. On the following lines we proof that this situation is not possible by proving that given $\tau_{A\mu}$ within $\tau_{A\rho} < \tau_{A\mu} < \tau_{A\pi}$ there is not a value of $\tau_{B\mu}$ greater than $\tau_{B\pi}$.

Proof. Suppose an arbitrary value of $\tau_{A\mu}$ and the corresponding $\tau_{B\mu}$ value, for all possible values of T_{lostA} and T_{lostB}. Equations (7.35) and (7.36) show the value of $\tau_{A\mu}$ and $\tau_{B\mu}$ calculated as on section 7.4.1.

$$\tau_{A\mu} = \left\lceil \frac{T_{lostB} - T_{lostA} + \gamma_{BA} - \Delta_B}{\Delta_A} \right\rceil \Delta_A \tag{7.35}$$

$$\tau_{B\mu} = T_{lostB} - T_{lostA} + \left\lceil \frac{T_{lostB} - T_{lostA} + \gamma_{BA} - \Delta_B}{\Delta_A} \right\rceil \Delta_A \tag{7.36}$$

Now we find the constrains imposed by the range of possible values of τ_A.

- $\tau_{A\mu} > \tau_{A\rho}$

$$T_{lostA} - T_{lostB} + \gamma_{AB} < \alpha' \gamma_{BA} + (1 - \alpha)\gamma_{AB} - \Delta_B \tag{7.37}$$

- $\tau_{A\mu} < \tau_{A\pi}$

$$T_{lostB} - T_{lostA} < \alpha \gamma_{AB} - \alpha' \gamma_{BA} + \Delta_B \tag{7.38}$$

Supposing there is a $\tau_{B\mu} > \tau_{B\pi}$, then equation (7.39) must be true.

$$T_{lostB} - T_{lostA} + \left\lceil \frac{T_{lostB} - T_{lostA} + \gamma_{BA} - \Delta_B}{\Delta_A} \right\rceil \Delta_A > \\ \alpha\gamma_{AB} - \alpha'\gamma_{BA} + \Delta_B + \left\lceil \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} - \Delta_A - \Delta_B}{\Delta_B} \right\rceil \Delta_B \tag{7.39}$$

Imposing the constrains defined on equation (7.37) and (7.38) into $\tau_{B\pi}$ we obtain equation (7.40).

$$\tau_{B\pi} > T_{lostB} - T_{lostA} + \lceil \frac{T_{lostB} - T_{lostA} + \gamma_{BA} - \Delta_B}{\Delta_A} \rceil \Delta_A \tag{7.40}$$

Equation (7.40) combined with equation (7.36) imposes that $\tau_{B\pi} > \tau_{B\mu}$ so the condition $\tau_{B\mu} > \tau_{B\pi}$ cannot be fulfilled. This ends this proof. □

7.4.2 Bidirectional traffic, One-Way failure

On this section, we consider scenarios in which node A and B exchange bidirectional traffic and a failure occurs in only one of the directions of the communication. As it will be seen, this case is a particularization of the analysis performed for the Bidirectional traffic, Two-Ways failure, in section 7.4.1.

Failure on the path from A to B

Equation (7.8), showed the expression which provides τ_{max} for a bidirectional traffic and Two-Ways failure. This equation applies when the first packet lost was sent by either A or by B. On the current scenario, B does not loose any packets since there is no failure on the path from B to A, hence $\tau_{B\theta}$, $\tau_{A\theta}$, $\tau_{A\sigma}$ and $\tau_{B\sigma}$ are not considered for this scenario. On the same way, equations in which the Send Timer is set on A are not considered, since A is always receiving packets and the Send Timer is being stopped and reset. Therefore equations $\tau_{A\pi}$, $\tau_{B\pi}$ and $\tau_{A\rho}$ are not considered. This reasoning yields to the fact that the τ_{max} for this scenario is equal to $\tau_{B\rho}$. Equation (7.41) shows the equation to consider on this scenario.

$$\tau_{max} = \gamma_{AB} - \Delta_A + \Delta_B \tag{7.41}$$

being this value of τ a maximal.

Failure on the path from B to A

Following the same reasoning as in previous section, for this scenario only $\tau_A\sigma$ must be considered. Hence equation (7.42) shows the value of τ_{max} to consider on this scenario.

$$\tau \leq \gamma_{BA} - \Delta_B + \Delta_A \tag{7.42}$$

being this value of τ a maximal.

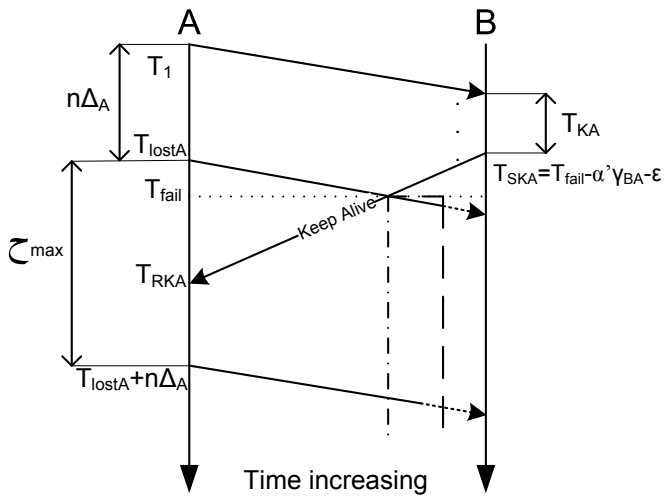


Figure 7.12: Worst Case scenario for Unidirectional traffic affected by a bidirectional failure

7.4.3 Unidirectional traffic, Two-Ways failure

Figure 7.12 presents the worst case for a unidirectional traffic flow affected by a bidirectional failure. This case occurs when a Keepalive message is sent on the latest possible instant before the failure. Therefore, the activation of the Send Timer when the next packet is sent produces the highest delay on τ. It is important to note that the time at which the Keepalive message is sent depends on the time at which node B receives a packet, hence the Keepalive message sending time on B depends on the traffic of the peer. Equation (7.43) presents the value of τ_{max} for this scenario.

$$\tau_{max} \leq \left\lceil \frac{T_{RKA} - T_{lostA}}{\Delta_A} \right\rceil \Delta_A \tag{7.43}$$

Due to the dependence between the Keepalive timer and the traffic sent by the peer, in order to calculate the value of τ_{max} we proceed on several stages. First we calculate the time at which peer A sends the packet which activates the Keepalive Timer on B (T_1, see figure 7.12). When the Keepalive timer expires on B, at time T_{SKA}, a Keepalive message is sent. T_{SKA} can be derived from T_1 by adding the propagation time and the T_{KA}. Then we can obtain the relationship between T_{lostA} and T_{SKA}. Once that the relation between T_{lostA} and T_{SKA} is found, the calculation of τ_{max} is done by finding the time at which the Keepalive message was received by A (T_{RKA}).
Equation (7.44) presents the mathematical representation of this relationships.

$$\begin{aligned} T_{SKA} &= T_{fail} - \alpha' \gamma_{BA} - \epsilon \\ T_1 &= T_{SKA} - T_{KA} - \gamma_{AB} \\ T_{lostA} &= T_1 + n\Delta_A \end{aligned} \tag{7.44}$$

The time at which the first lost packet is sent by A (T_{lostA}) occurs a given number (n) of Δ_A periods after the packet that started the Keepalive at B was sent (T_1). Note that T_{lostA} is

related with T_{fail} by the following equation.

$$T_{fail} - \alpha\gamma_{AB} \leq T_{lostA} < T_{fail} - \alpha\gamma_{AB} + \Delta_A \tag{7.45}$$

Then,

$$\begin{aligned} T_{lostA} &\geq T_{fail} - \alpha\gamma_{AB} \\ n\Delta_A &\geq T_{fail} - \alpha\gamma_{AB} - T_1 \\ n\Delta_A &\geq (1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} + T_{KA} \end{aligned} \tag{7.46}$$

$$\begin{aligned} T_{lostA} &< T_{fail} - \alpha\gamma_{AB} + \Delta_A \\ n\Delta_A &< T_{fail} - \alpha\gamma_{AB} + \Delta_A - T_1 \\ n\Delta_A &< (1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} + T_{KA} + \Delta_A \end{aligned} \tag{7.47}$$

Combining both equations, we obtain the value for T_{lostA}.

$$T_{lostA} = T_1 + \left\lfloor \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} + T_{KA}}{\Delta_A} + 1 \right\rfloor \Delta_A \tag{7.48}$$

The time at which the Keepalive is received is expressed as

$$T_{RKA} = T_{SKA} + \gamma_{BA} \tag{7.49}$$

τ_{max} corresponds to the difference between T_{RKA} and T_{lostA}, taking into account that the Send Timer starts on the next packet sent, as shown in equation (7.50).

$$\begin{aligned} T_{SKA} &= T_{fail} - \alpha'\gamma_{BA} - \epsilon \\ T_{RKA} &= T_{SKA} + \gamma_{BA} \\ T_1 &= T_{SKA} - T_{KA} - \gamma_{AB} \\ T_{RKA} &= T_{fail} + (1-\alpha')\gamma_{BA} - \epsilon \\ T_1 &= T_{fail} - \alpha'\gamma_{BA} - \epsilon - T_{KA} - \gamma_{AB} \\ \tau_{max} &= \left\lceil \frac{R_{TT} + T_{KA} - \lfloor \frac{(1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA} + T_{KA}}{\Delta_A} + 1 \rfloor \Delta_A}{\Delta_A} \right\rceil \Delta_A \end{aligned} \tag{7.50}$$

This value of τ_{max} is a maximal.

7.4.4 Unidirectional traffic, One-Way failure on data path

Figure 7.13 presents the worst case for an unidirectional traffic flow affected by a failure just on the data path. This case occurs when the Keepalive Timer on peer B is started by the latest possible data packet sent by peer A. After a Keepalive Timer period, a Keepalive message is sent from B to A, resetting the Send Timer on A.

$$\begin{aligned} T_{RKA} &= T_{fail} - \alpha\gamma_{AB} + \gamma_{AB} + T_{KA} + \gamma_{BA} - \epsilon \\ T_{lostA} &= T_{fail} - \alpha\gamma_{AB} + \Delta_A - \epsilon \\ \tau_{max} &= \left\lceil \frac{T_{RKA} - T_{lostA}}{\Delta_A} \right\rceil \Delta_A \end{aligned} \tag{7.51}$$

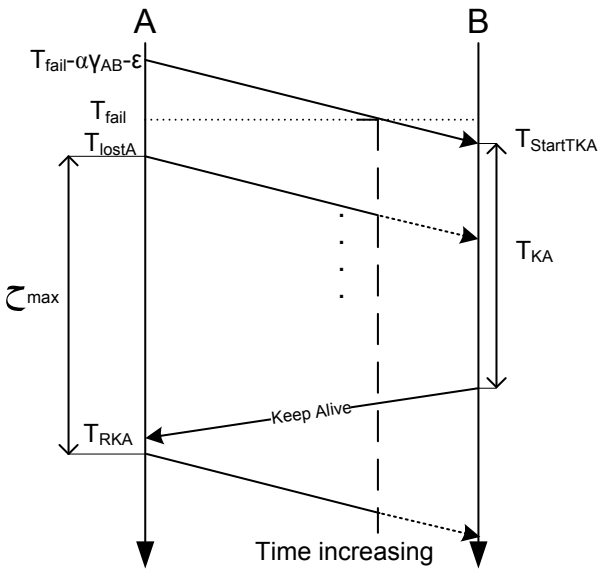


Figure 7.13: Worst Case scenario for Unidirectional traffic affected by a failure on data path

Parameter	Initial Value	Ending Value
Δ_A	1ms	200ms
Δ_B	1ms	200ms
γ_{AB}	1ms	100ms
γ_{BA}	1ms	100ms
α	0	1
α'	0	1

Table 7.1: Traffic Characteristics for random exploration

Equation (7.52) shows the value of τ_{max} for this case, being this value of τ_{max} a maximal.

$$\tau = \left\lceil \frac{R_{TT} + T_{KA} - \Delta_A}{\Delta_A} \right\rceil \Delta_A \tag{7.52}$$

7.4.5 τ Simulation Results

In order to validate the results presented before, an extensive search of maximum values for τ has been performed.
First, a simulator of the REAP's failure detection mechanism for the communication of two nodes has been implemented on Matlab. A given experiment is defined by the type of communication, failure type, and an specific set of values for Δ_A, Δ_B, γ_{AB}, γ_{BA}, α and α'. For each experiment, the starting time for the periodic data sending in A (B) is varied in fractions of the sending period Δ_A (Δ_B), being tested all the different combinations of the defined starting times at A and B, for a given failure time and the corresponding τ is obtained. In order to obtain a more precise value for the maximum of τ, further simulations were performed with starting points close to the ones in which the higher τ value was obtained, using in this time smaller variations. Many experiments have been run for each scenario defined

by the type of communication and the type of failure. For each of these scenarios the numerical parameters that define an experiment (Δ_A, Δ_B, γ_{AB}, γ_{BA}, α and α') have been generated using two approaches. In the first approach, we have generated a set of values for each parameter by defining a starting value that is incremented by a fixed step. Then, we have simulated all the configurations resulting from the combinations of these values (around 5500 samples for each Bidirectional Traffic scenario and 1400 sample for each Unidirectional Traffic scenario). In the second approach, we have generated randomly the values of the parameters (200 samples for each scenario), supposing a uniform distribution among fixed initial and final values (Table 7.1). Once the maximum simulation result of τ for a given experiment has been obtained, this value is compared with the expected theoretical result. In particular, the results provided by equations:

- Equation (7.8) for the Bidirectional traffic, Two-Ways failure case.
- Equations (7.41) and (7.42) for the Bidirectional traffic, One-Way failure case.
- Equation (7.50) for the Unidirectional traffic, Two-Ways failure.
- Equation (7.52) for the Unidirectional Traffic, One-way failure on the data path respectively.

In all cases, the difference between the theoretical analysis and the simulated model is 0 when the value of τ corresponds to a maximal, being the theoretical model able to model without error the value of τ_{max}. When the theoretical result is a supremum, the simulator provides results whose differences with the theoretical predictions can be made arbitrarily small by reducing the step used for the variation of the sending times at A and B. Further detail in the simulation results can be obtained from [92].

7.5 Upper bound for the Recovery Time regardless of the Location and Type of the failure

On this section we provide an upper bound for the $T_{recovery}$ independently of the point and type of failure for the Bidirectional and Unidirectional Traffic. First an upper bound for τ_{max} regardless the point of failure is obtained for the scenarios that depended on the α and α' parameters, that were the Bidirectional traffic, Two-Ways failure, and the Unidirectional Traffic Two-Ways Failure. Then, we provide an upper bound for $T_{recovery}$ in the Bidirectional Traffic and in the Unidirectional Traffic scenarios independent on the failure type or location.

7.5.1 Upper bound for τ regardless the location of the failure: Bidirectional traffic, Two-Ways failure

A supremum for τ for Bidirectional traffic, Two-Ways failure, was provided in equation (7.8). In order to obtain a compact expression for an upper bound that does not depend on the location of the failure (i.e. on α or on α'), we first apply the inequalities $x + 1 \geq \lceil x \rceil$

and $x - 1 \leq \lfloor x \rfloor$ to obtain the following equation:

$$\begin{aligned} max\Big[&min\big(\alpha\gamma_{AB} + (1-\alpha')\gamma_{BA} + \Delta_A, \gamma_{AB} + \Delta_B - \Delta_A\big), \\ &min\big(\alpha'\gamma_{BA} + (1-\alpha)\gamma_{AB} + \Delta_B, \gamma_{BA} + \Delta_A - \Delta_B\big), \\ &min\big(\gamma_{AB} + \Delta_B - \Delta_A, R_{TT} - \alpha'\gamma_{BA} - (1-\alpha)\gamma_{AB} + \Delta_A\big), \\ &min\big(\gamma_{BA} + \Delta_A - \Delta_B, R_{TT} - \alpha\gamma_{AB} - (1-\alpha')\gamma_{BA} + \Delta_B\big)\Big] \end{aligned} \tag{7.53}$$

It is trivial to realize that the values of α and α' that maximize equation (7.53) are $\alpha = 0, \alpha' = 1$ and $\alpha = 1, \alpha' = 0$.
Therefore,

$$\begin{aligned} \tau_{upp} = max\Big[&min(R_{TT} + \Delta_A, \gamma_{AB} + \Delta_B - \Delta_A), \\ &min(R_{TT} + \Delta_B, \gamma_{BA} + \Delta_A - \Delta_B), \\ &min(\gamma_{AB} + \Delta_B - \Delta_A, R_{TT} + \Delta_A), \\ &min(\gamma_{BA} + \Delta_A - \Delta_B, R_{TT} + \Delta_B)\Big] \end{aligned} \tag{7.54}$$

Eliminating the terms that are duplicated, we obtain

$$\begin{aligned} \tau_{upp} = min\Big[&max\big(\gamma_{BA} + \Delta_A - \Delta_B, \gamma_{AB} + \Delta_B - \Delta_A\big), \\ &max\big(R_{TT} + \Delta_A, R_{TT} + \Delta_B\big)\Big] \end{aligned} \tag{7.55}$$

On the same way, an upper bound for the value of τ_c (τ on the correspondent node) is shown on equation (7.56).

$$\begin{aligned} \tau_{uppC} = max\Big[&max\big(\gamma_{BA} + \Delta_A - \Delta_B, \gamma_{AB} + \Delta_B - \Delta_A\big), \\ &max\big(R_{TT} + \Delta_A, R_{TT} + \Delta_B\big)\Big] \end{aligned} \tag{7.56}$$

Note that the simplifications done to calculate the upper bound and the conditions of the supremum on equations (7.23) and (7.25), let us assure that $\tau_{max} \leq \tau_{upp} \leq \tau_{max} + max(\Delta_A, \Delta_B)$.

7.5.2 Upper bound for τ regardless the location of the failure: Unidirectional traffic, Two-Ways failure

In a similar way to section 7.5.1, we can obtain upper bound equation (7.50), that provided a maximum for τ for Unidirectional traffic, Two-Ways failure to obtain an equation that does not depend on the location of the failure.

$$\tau_{upp} < R_{TT} - \big((1-\alpha)\gamma_{AB} + \alpha'\gamma_{BA}\big) + \Delta_A \tag{7.57}$$

On this case, equation (7.57) is maximized by setting $\alpha = 1$ and $\alpha' = 0$. Finally the upper bound value for the τ for this case is presented on equation (7.58).

$$\tau_{upp} < R_{TT} + \Delta_A \tag{7.58}$$

7.5.3 Upper bound for the Recovery Time for Bidirectional Traffic

We now aim to provide an expression for the Recovery Time regardless the type and location of the failure for Bidirectional Traffic. In section 7.5.1 we have obtained an expression for τ for Bidirectional traffic, Two-Ways failure, that is independent of the location of a failure. We had also obtained two expressions that characterize τ for the case of Bidirectional traffic, One-Way failure (equations (7.41) and (7.42)) that already were independent of the location of the failure. The maximum of these expressions correspond to the One-Way Failure case. Therefore the upper bound for τ for Bidirectional Traffic is

$$\tau_{upp} = max(\gamma_{BA} + \Delta_A - \Delta_B, \gamma_{AB} + \Delta_B - \Delta_A) \tag{7.59}$$

Combining equation (7.59) and equation (7.6), we obtain the upper bound for the recovery time:

$$T_{recovery} < T_{RTx} + R_{TT} + max(\gamma_{AB}, \gamma_{BA}) + T_{Send} + \tau_{upp} \tag{7.60}$$

7.5.4 Upper bound for the Recovery Time for Unidirectional Traffic

From section 7.5.2, the upper bound of τ for the case of Unidirectional traffic, Two-Ways failure corresponds to equation (7.58). The value of τ for Unidirectional Traffic, One-Way failure does not depend on the point of failure and is presented on equation (7.52). Then, the upper bound of $T_{recovery}$ for the Unidirectional Traffic case is

$$\begin{aligned} \tau_{upp} &= \left\lceil \frac{R_{TT} + T_{KA} - \Delta_A}{\Delta_A} \right\rceil \Delta_A \leq R_{TT} + T_{KA} \\ T_{recovery} &< T_{RTx} + 2R_{TT} + T_{send} + \tau_{upp} \end{aligned} \tag{7.61}$$

7.5.5 A case study of the applicability of the results

We illustrate the previous results with a case study: Suppose a bidirectional VoIP application using a codec which generates a packet each 30 ms. The propagation time for all paths is upper bounded by 150 ms (symmetrical case). In this scenario, equation (7.60) provides an upper bound for the time required to start the Send Timer (τ) of 150 ms for the first peer detecting the failure. Supposing the first path explored after the current one is working, the time required to recover from a failure corresponds to $0.5 + 0.3 + T_{Send} + 0.15 + 0.15$ seconds. Once the time required to start the Send Timer and to find a working path is known, the Send Timer can be set according to the requirements imposed by the application. A final check should be performed to be sure that the loss of a small number of packets for other reasons than an outage of the path does not trigger the exploration process, i.e. check that $\frac{T_{send}}{\Delta_A}$ and $\frac{T_{send}}{\Delta_B}$ are larger than a small value such as 3 or 4. Note that a transient event such as temporal congestion in the path could create an unavailability of the path for a period of time that REAP detects as a path failure. However, it could be a good strategy for applications with tight constraints in terms of the maximum time at which the communication is unavailable to check for other possibly better paths when a communication problem occurs, regardless the nature of it (long-term outage or just increased congestion). With these considerations, if the designer of the VoIP application considers that a failure should be recovered in less than 1.5 seconds, a T_{send} value of 0.4 seconds should be set. Note that in

this case 13 data packets have to be lost for the expiration of the Send Timer. By this simple example we provide a way for the application to configure the REAP timers according to the desired failure recovery time.
On the other hand if another application with the same characteristics but unidirectional traffic is affected by an outage on the data path, the time required to detect the failure depends on the Keepalive Timer. It is worth to notice that the value of the Keepalive timer has an impact on the signaling generated by this protocol. Suppose an application requiring a Recovery Time of at most two seconds. Suppose we choose to set up the Keepalive timer to five packets, the corresponding value of τ is 0.42 seconds (equation (7.61)). With the information of the exploring time and τ, the Send Timer is computed to meet the application requirements as 16 packets (480 ms). The overall time required to recover from the failure is $0.42+0.3+0.3+0.5+0.48 = 2\ sec$ (equation (7.61)), that complies with the requirements imposed by the application.
With this result we can also think in algorithms that dynamically adapt REAP timers accordingly to measured parameters as delay or packet rate.

7.6 Failure Recovery effect on Upper Layers protocols

Previous sections have been devoted to the analytical characterization of the Failure Discovery and Path Exploration protocol (REAP). The results presented on previous sections focus on layer 3 recovery not taking into account the possible interactions with mechanisms of upper layers. In this section we simulate the REAP protocol with the OPNET[1] tool and we analyze the interactions with a particular relevant upper layer case that is TCP.

7.6.1 Simulation Setup

In this section we present the scenario used to test the path failure detection functionality of the REAP protocol. Figure 7.14 shows two nodes, Node A and B, each one with two interfaces and an IPv6 address configured on each interface. All simulations have been performed by establishing a communication through the pair (IP_{A1}, IP_{B1}). All traffic exchanged between these IP addresses goes through Cloud 1 and 2. At a certain time, the link connecting Cloud 1 and 2 fails, this is detected by REAP and after a path exploration, the communication is continued using the IP pair (IP_{A2}, IP_{B2}). Tests performed involve the TCP protocol. The Windows Server 2003 TCP stack[2] model defined in OPNET has been used.
The RTT in both paths is the same, it has been implemented as a normal distribution with mean 80ms and 20ms variance. The failure event occurs at a time defined by an uniform distribution between 75 and 125 seconds. All simulations have been run for 250 seconds, the presented results are the average of 45 samples. The real values are within $\pm 10\%$ (on the worst case) of the estimated values with a confidence interval of 95%.

In order to find the values for the REAP timers that optimize the behavior of TCP when a path failure occurs, several measures have been performed. The main metric used through

[1] OPNET University Program, http://www.opnet.com/services/university/
[2] http://technet2.microsoft.com/WindowsServer/

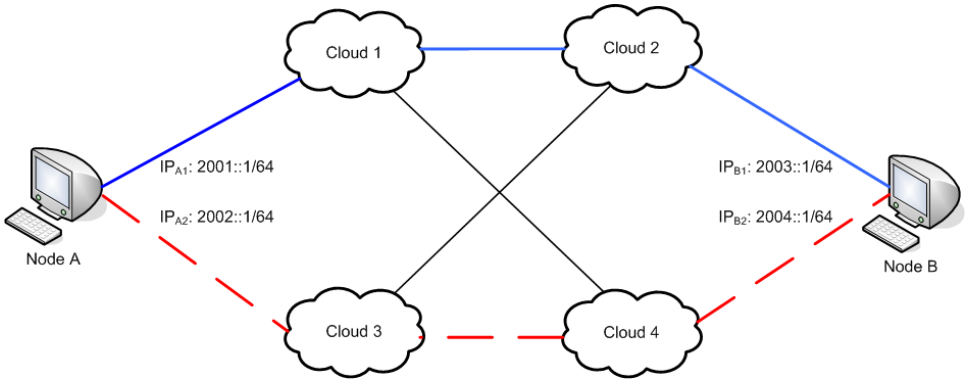


Figure 7.14: Simulated Scenario

the analysis is the *Application Recovery Time*. This metric is defined as the difference in time between the last packet arriving through the old IP locators (addresses) and the first packet arriving through the new ones. This metric accurately measures the time to recover from a path failure when there is continuous traffic. Note that this time is a measurable approximation to the recovery time defined in previous sections.

TCP incorporates several characteristics such as congestion control and reliability that determines the resulting performance when a valid path is provided as a result of the REAP operation. To understand the behavior of applications using TCP two traffic types have been considered, a FTP download from a server and a telnet session showing sparse traffic exchange. With these two traffic types the behavior of applications with high traffic demands and applications with low traffic profiles are considered.

7.6.2 TCP behavior

FTP Application

Figure 7.15 shows the Application Recovery Time achieved while varying the T_{Send} timer. Note that the results for TCP traffic are not linear with the T_{Send} parameter as the expressions presented in 7.5 are. This behavior is due to the mechanisms implemented in TCP for congestion detection and avoidance, in particular dependent on the retransmission timeout of TCP. Such mechanisms have not been taken into account in the analytical study performed in sections 7.2 to 7.5. TCP interprets a retransmission timeout as an indication of congestion in the network, so it uses an exponential back-off to retransmit the packets to avoid increasing the congestion. This mechanism affects the Application Recovery Time, since although the path has been reestablished, the packets will not be retransmitted until the retransmission timeout expires. To show a detailed explanation of this behavior we present figure 7.16(a). Figure 7.16(a) presents, for a given experiment ($T_{Send} = 10sec$), the Retransmission Timeout, Congestion Window and traffic sent through both paths. Traffic starts being sent through the primary path, until the link fails. At this moment the congestion window decreases and the retransmission timer increases. When the path exploration mechanism ends, the retransmission timer set up to 8 seconds has not expired. When it expires,

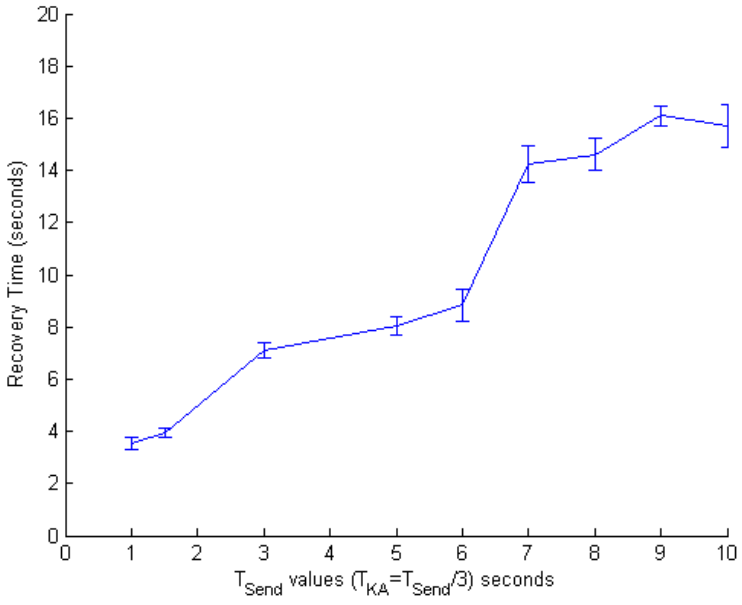
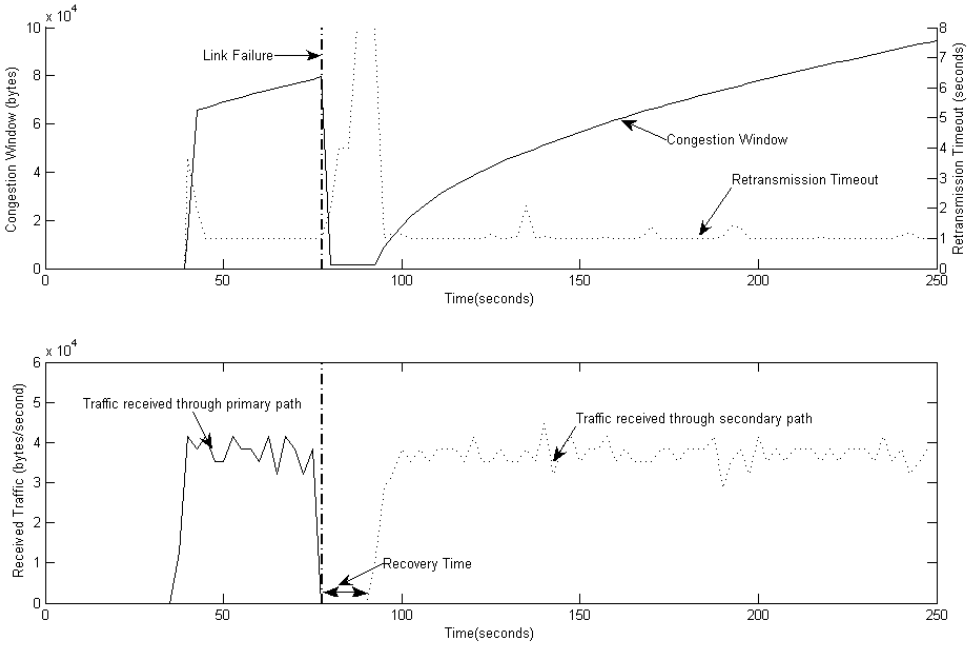
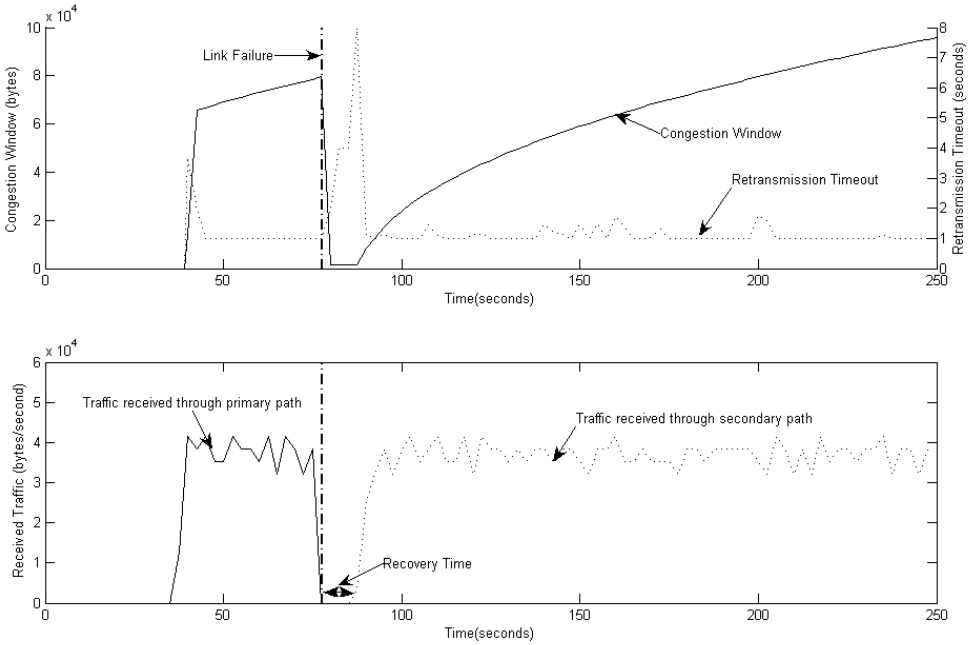


Figure 7.15: TCP Recovery Time

packets are sent according to the slow start policy set for TCP. Figure 7.17 shows the difference in time between the arrival of a packet in a connection with a failure and the arrival of the same packet if no failure in the path occurs. As can be observed, packets suffer a big delay when the link fails (this delay is equivalent to the time needed to discover the failure and complete a path exploration mechanism), and then it remains roughly constant. This effect is due to the increase in the congestion window after the communication is recovered, packets will start to be sent faster until the congestion window reaches its top, after this packets are sent in a constant way, this behavior can be observed in figures 7.16(a) and 7.17. Due to the explanation presented above, we argue that the stair shaped graph in figure 7.15 is caused by the impact of the back-off mechanism of the retransmission timer of TCP. Figure 7.18, presents the back-off mechanism used by TCP to set up the retransmission timer. As the number of retransmissions increases, the retransmission timer duplicates its value. We argue that as the T_{Send} varies, the instant in time when the path is recovered falls in one of the steps presented in figure 7.18, this is the cause of the differences in time presented in figure 7.15. To improve the performance, we propose to reset the retransmission timer of TCP after a new path is chosen for the communication (figure 7.16(b)). Notice that this is not only more efficient, but also appropriate as the retransmission timer value is dependent on the properties of the path. In the simulator, we implemented a hook in the TCP stack to allow REAP to reset the retransmission timer forcing TCP to start retransmitting packets immediately. The experimental results of this proposal are presented in figure 7.19. This figure presents the previous results of the Application Recovery Time of TCP along with the Application Recovery Time obtained when the Retransmission Timer of TCP is reseted, for easier comparison. As expected, when resetting the Retransmission Timer, the relation between the TCP Recovery Time and T_{Send} is linear, as predicted by the expressions obtained



(a) Normal TCP operation



(b) TCP operation resetting the retransmission timeout

Figure 7.16: TCP behavior explanation

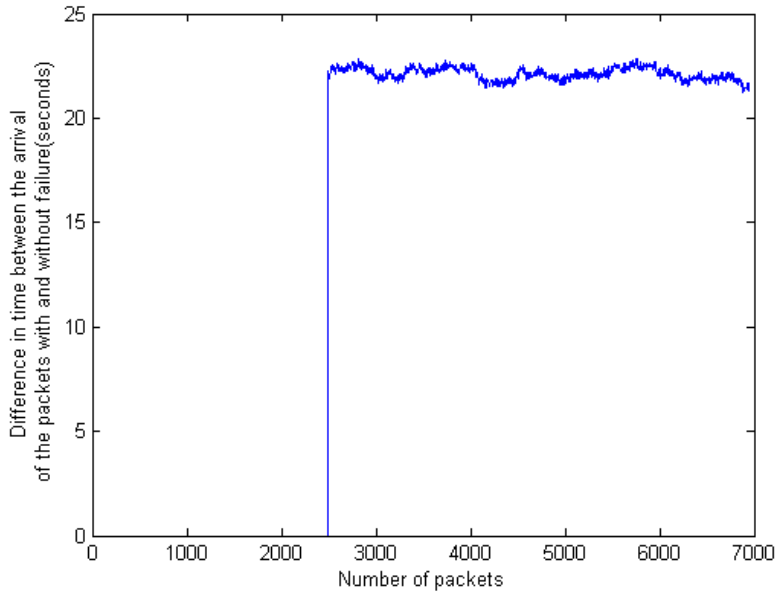


Figure 7.17: Difference in time between packets in a communication with path failure and without path failure

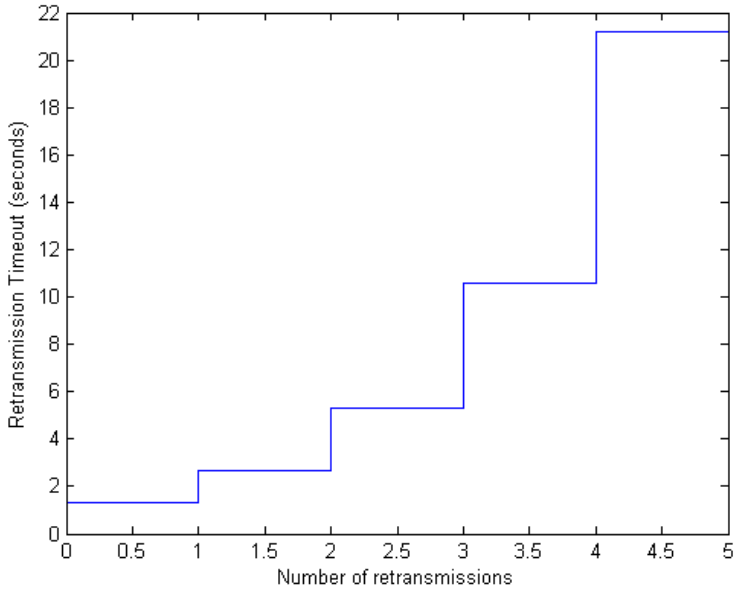


Figure 7.18: TCP Retransmission Timeout

in section 7.5.

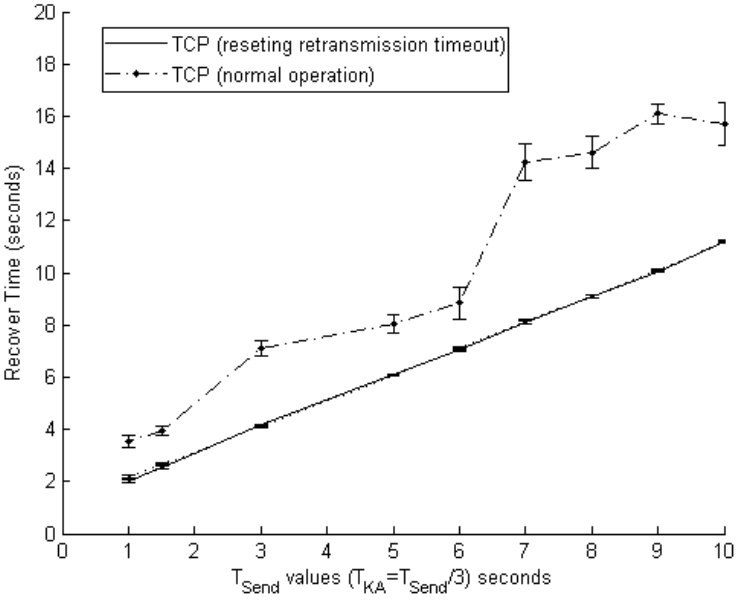


Figure 7.19: Standard TCP vs. TCP (resetting the retransmission timer) Recovery Time

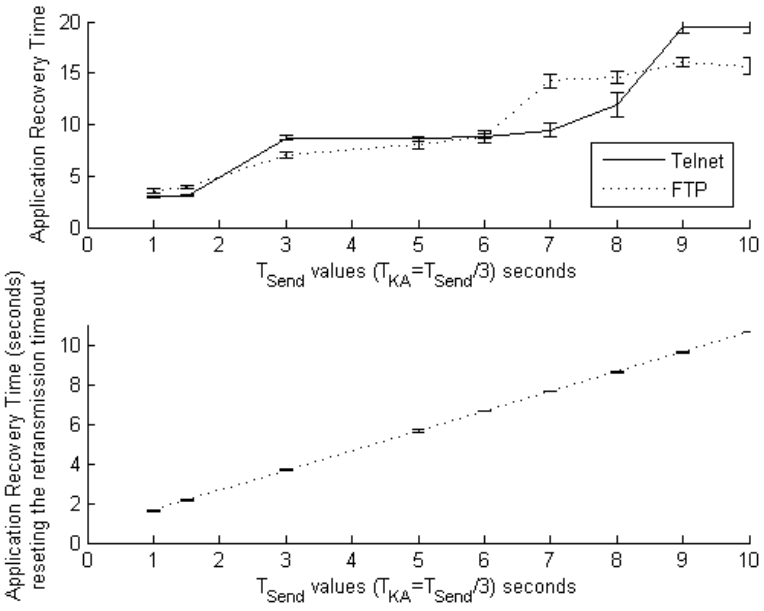


Figure 7.20: Recovery time in a telnet application

Telnet Application

To conclude the TCP study, an application with low data traffic has been analyzed. The chosen application is Telnet, in which usually long periods of time without packet transmis-

sion occurs. The design of REAP tries to minimize signaling overhead, so no Keep Alive probing is performed when no upper layer traffic is exchanged, due to this behavior, REAP will notice the failure after a time, defined by T_{Send}, of the first packet sent after the failure. To show this behavior figure 7.20 is presented. The Application Recovery Time metric, refers to the time elapsed between the first packet (using the old locators) sent after the failure and the first packet sent using the new locators. On this time period, the failure discovery and path exploration mechanisms are performed. The recovery procedure start time offset depends on the time between the path failure and the time when the application first tries to send a packet, but this offset is not important since the application is not affected by the failure because it was not trying to exchange any traffic. Figure 7.20 presents a similar trend to figure 7.15, presented on this figure for comparison purposes. The impact on the Application Recovery time of resetting the retransmission timer of TCP is shown in figure 7.20. As can be seen the effect is similar to the one presented on figure 7.19, being it a noticeable decrease on the Recovery Time of the application.

7.7 Conclusion

In this chapter an exhaustive analytical study of the time required by REAP to recover from a path failure has been performed. We also present a simulation study exploring the interaction of REAP and the TCP transport protocol, together with a possible modification to the TCP stack which enables to take advantage of the REAP protocol to provide a faster Recovery Time, as seen from TCP applications.
The main focus has been on characterizing the $T_{recovery}$ figure of merit for bidirectional and unidirectional communication types. However, separate results for the failure detection process (mainly characterized by the τ parameter) and the exploration process have been obtained. These separate results could be used for characterizing other architectures in which only the failure detection mechanism of REAP were adopted. Supremum values (i.e. optimal upper bounds) have been provided for the characterization of τ and the Recovery Time, except for the final expressions in which compact upper bounds independent of the failure type or location are provided. The proposed expressions depend on the propagation times of the paths involved, and on the values of the Keepalive and Send Timers. These timers can be adjusted at will for each communication to comply with a given $T_{recovery}$ in a particular scenario. Our architecture takes benefit from these results by allowing the proper configuration of the REAP timers. Through this configuration the terminals are able to detect failures in a timely manner, reacting with enough time to prevent broken connections and general failures in the communication.

Further work is required to extend the model to consider the case in which more than one path is explored sequentially until a working path is found. This case results in transitions not considered in this work, making the analysis more complex. Additionally, it requires considering the exponential back-off mechanism defined to increase the period at which Probe messages are being sent. Nevertheless, it can be very inefficient to configure REAP to recover in bounded times from complex failure situations affecting to several alternative paths and, if this is required, concurrent exploration of the possible alternative paths seems the best option. Another research area would be to extend the study performed for static

configurations of REAP and stable communication parameters to scenarios in which the communication path conditions may vary and REAP adapts to this situation in order to comply to a given recovery time. Finally, it would be possible to apply the methodology devised in our work to other failure detection protocols with some similarities to the failure detection module of REAP, such as Bidirectional Forwarding Detection (BFD) [93] or Neighbor Unreachability Detection (NUD) [27].

Part VI

Conclusions and Future Work

Chapter 8

Conclusions and Future Work

In this thesis we have presented an architecture which provides to multi-technology terminals: i) efficient mobility support using IEEE 802.21 in heterogeneous access networks and ii) capabilities in order to take advantage of multihoming to increase terminals' robustness to failures in the links used for their communications.

In the following lines, the contributions of this thesis are summarized, along with the publications of this work:

1. We have performed a detailed study of the upcoming IEEE 802.21 standard. This study highlights the importance of this technology in the current networking environment, and its possibilities. This study has been published in [94].
2. We have studied the integration of IEEE 802.21 in a multi-technology terminal, exploring the proper configuration of the parameters used to decide the best handover timing. We have proposed a way of implementing the abstraction layer provided by IEEE 802.21 in a terminal, by means of a simulator implementation. Using the IEEE 802.21 framework, we have designed a handover decision algorithm that using two WLAN signal level thresholds and for a $3G \leftrightarrow WLAN$ environment, is able to favor WLAN utilization or service continuity (minimizing packet loss) depending on its configuration. This have showed the flexibility of the IEEE 802.21 model for implementing handover policies. We have also provided the proper configuration of the thresholds used to trigger the handovers in order to maximize the utilization time of the target technology while minimizing the disruption (losses) of the communication. This work has been published in [95].
3. We have analyzed the proper configuration of the thresholds for different terminal speeds, analyzing the effect in this configuration of the delay in the links. We proposed configurations achieving seamless handovers for different terminal speeds and algorithms able to cope with this changes. In this study we have also analyzed the effect of high WLAN signal fluctuations in the algorithms used to evaluate the thresholds, providing an efficient way of extracting the signal level from different samples in environments with high signal variation due to speed or other causes. This work has been published in [96].

4. We have showed that network initiated handovers can significantly increase network utilization. We have identified scenarios for network deployment to maximize the benefit from network initiated handovers, such as overlapping areas, and asymmetries due to traffic patterns or different access technologies. This work is published in [97]. Following this discussion, we proposed the integration of the Network Controlled Handovers paradigm in IEEE 802.21, analyzing factors such as signaling overhead and the delay introduced by the signaling. We have also proposed algorithms on terminals and the network to control handovers, under network control, avoiding race conditions. This work has been published in [98].

5. We have provided an analysis of the REAP protocol, which enables the terminal to detect failures in its communications and recover from them. We have performed the analytical characterization of the time required by the protocol to detect a failure in the communication. This is a fundamental result since, through this characterization, REAP can be configured to detect and recover from a failure in a target time, so for a given scenario (RTT, inter-packet rates) we provide the REAP configuration to achieve a certain recovery time. This work has been submitted to a journal [99]. We have to consider that certain upper layers can have mechanisms that interfere with the time of recovery, for example, an upper layer can refrain from transmitting during some time after a packet loss. TCP is a particular interesting example of this. We have analyzed by simulation the interaction between REAP and TCP in [100] and proposed a crosslayer mechanism to improve the recovery time of TCP when using REAP.

Finally, related with this thesis, we have also made some other contributions. From this remaining contributions it is worth to stress [14] and [15], which correspond to contributions to the IEEE 802.21, and also [101] and [102] which correspond to the continuation of the work started in [97] and [98] .

Once the main contributions of this thesis have been presented, in the following lines we present the future topics of research that this thesis opens:

- Analysis and design of more complex algorithms for the management of terminals in Network Initiated Mobility scenarios. The algorithms presented in this thesis only take into account the load of the APs. It is important to work on more complex algorithms taking into account different technologies and their characteristics, QoS constrains, cost issues, and overall network utilization metrics, to perform a better point of attachment selection for the mobile nodes while maximizing network usage. With this complex scenarios, the coordination between mobile initiated and network initiated handovers will be also more complex, and will require detailed study.

- Use of an IEEE 802.21 inspired approach for the design of an abstraction layer for wireless heterogeneous mesh networks. One of the future objectives of this work is to impact in the IEEE 802.21 working group with the aim of extending the IEEE 802.21 MIHF to support wireless heterogeneous mesh networks.

- Extend the behavior of REAP to dynamically adapt the timers it uses, in function of the variations of the RTT and the inter-packet rate. Using as starting point the analytical model developed in this thesis, the REAP timers could be modified dynamically

in function of several parameters in such a way that the recovery time is adjusted to a specific target. Attention is needed to the coordination of both sides of the communication. With the work on this thesis we have the basis for this solution, but extensive experimentation is needed to validate its practical use.

- Extend the analytical model of REAP to a probabilistic model, taking into account the variance of all the parameters. We also want to crosscheck this new model with a real implementation of REAP to validate it.

References

[1] "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services (Draft 07)." IEEE August 2007.

[2] "Internet Engineering Task Force." [Online]. Available: http://www.ietf.org/

[3] "3rd Generation Partnership Project (3GPP)." [Online]. Available: http://www.3gpp.org/

[4] "3rd Generation Partnership Project 2 (3GPP2)." [Online]. Available: http://www.3gpp2.org/

[5] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6." RFC3775, RFC Editor United States, 2004.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol." RFC3261, RFC Editor United States, 2002.

[7] "Mobility for IP: Performance, Signaling and Handoff Optimization." [Online]. Available: http://www.ietf.org/html.charters/mipshop-charter.html

[8] T. Melia, E. Hepworth, S. Sreemanthula, Y. Ohba, G. Vivek, J. Korhonen, R. Aguiar, and S. Xia, "Mobility Independent Services: Problem Statement." RFC5164, RFC Editor United States, March 2008.

[9] A. Rahman and U. Olvera-Hernandez and M. Watfa, "Transport of Media Independent Handover Messages Over IP." Internet Engineering Task Force, draft-rahman-mipshop-mih-transport-03 (work in progress), July 2005.

[10] E. Hepworth, R. Hancock, S. Sreemanthula, and S. Faccin, "Design Considerations for the Common MIH Protocol Functions." Internet Engineering Task Force, draft-hepworth-mipshop-mih-design-considerations-01 (work in progress), October 2006.

[11] S. Sreemanthula, S. Faccin, E. Hepworth, and G. Daley, "Problem Statement and Requirements for Event and Command Services in Media Independent Handovers." Internet Engineering Task Force, draft-sreemanthula-es-cs-problem-02 (work in progress), June 2006.

[12] A. Vidal, T. Melia, and A. Banchs, "Proxy functionality for Event Service and Command Service," November 2006. [Online]. Available: http://www.ieee802.org/21/doctree/2006-11_meeting_docs/21-06-0795-00-0000-ES_CS_Proxy.doc

[13] A. Vidal and T. Melia and A. Banchs, "Support for Centrally Coordinated Network Initiated Handovers," November 2006. [Online]. Available: http://www.ieee802.org/21/doctree/2006-11_meeting_docs/21-06-0783-00-0000-centralized_NIHO.doc

[14] A. Vidal, T. Melia, A. Banchs, and A. de la Oliva, "MIH Users Event Service," January 2007. [Online]. Available: http://www.ieee802.org/21/doctree/2007-01_meeting_docs/21-07-0009-00-0000-MIH_User_generated_events.doc

[15] ——, "Multitechnology Mesh Scenario," March 2007. [Online]. Available: http://www.ieee802.org/21/doctree/2007-03_meeting_docs/AdHoc_Feb07/21-07-0065-00-0000-Multitechnology_mesh_scenario.doc

[16] L. Kazovsky, G. Khoe, and M. van Deventer, "Future telecommunication networks: major trend projections," *Communications Magazine, IEEE*, vol. 36, no. 11, pp. 122–127, 1998.

[17] U. oA, "Forum Report No. 8: The Future Mobile Market–Global trends and developments with a focus on Western Europe. UMTS Forum März 1999."

[18] W. Mohr and W. Konhauser, "Access network evolution beyond third generation mobile communications," *Communications Magazine, IEEE*, vol. 38, no. 12, pp. 122–133, Dec 2000.

[19] S. Alexander and R. Droms, "DHCP Options and BOOTP Vendor Extensions." RFC 2132,RFC Editor United States, 1993.

[20] P. Mockapetris, "Domain names-concepts and facilities." RFC1034, RFC Editor United States, 1987.

[21] ——, "Domain names-implementation and specification." RFC1035, RFC Editor United States, 1987.

[22] Hesham Soliman, *Mobile IP: Mobility in a Wireless Internet*. Addison Wesley, 2004.

[23] C. Perkins, S. Alpert, and B. Woolf, *Mobile IP; Design Principles and Practices*. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA, 1997.

[24] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson, "Stream Control Transmission Protocol." RFC2960, RFC Editor United States, 2000.

[25] R. Stewart and C. Metz, "SCTP: new transport protocol for TCP/IP," *Internet Computing, IEEE*, vol. 5, no. 6, pp. 64–69, 2001.

[26] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification." RFC2460, RFC Editor United States, 1998.

[27] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)." RFC2461, RFC Editor United States, 1998.

[28] J. Abley, P. Savola, and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6." RFC5095, RFC Editor United States, 2007.

[29] R. Wakikawa and T. Ernst and K. Nagami and V. Devarapalli, "Multiple Care-of Addresses Registration." Internet Engineering Task Force, draft-ietf-monami6-multiplecoa-05 (work in progress), January 2008.

[30] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)." RFC4140, RFC Editor United States, 2005.

[31] E. R. Koodli, "Fast Handovers for Mobile IPv6." RFC4068, RFC Editor United States, 2005.

[32] J. Kempf, "Goals for Network-based Localized Mobility Management (NETLMM)." RFC4831, RFC Editor United States, 2006.

[33] ——, "Problem Statement for Network-Based Localized mobility Management (NETLMM)." RFC4830, RFC Editor United States, 2007.

[34] Iljitsch Van Beijnum, *BGP: Builiding Reliable Networks with the Border Gateway Protocol*. Ed O'Reilly, 2002.

[35] Y.Rekhter and T.Li, "A Border Gateway Protocol 4 (BGP-4)." RFC1771, RFC Editor United States, 1995.

[36] "Site Multihoming by IPv6 Intermediation." [Online]. Available: http://www.ietf.org/html.charters/shim6-charter.html

[37] E. Nordmark and M. Bagnulo, "Level 3 multihoming shim protocol." Internet Engineering Task Force, draft-ietf-shim6-proto-09 (work in progress), November 2006.

[38] J. Abley and M. Bagnulo, "Applicability Statement for the Level 3 Multihoming Shim Protocol(shim6)." Internet Engineering Task Force, draft-ietf-shim6-applicability-03 (work in progress), July 2007.

[39] J. Arkko and I. van Beijnum, "Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming." Internet Engineering Task Force, draft-ietf-shim6-failure-detection-11 (work in progress), January 2008.

[40] R. Draves, "Default Address Selection for Internet Protocol version 6 (IPv6)." RFC3484, RFC Editor United States, 2003.

[41] M. Bagnulo, "Updating RFC 3484 for multihoming support." Internet Engineering Task Force, draft-bagnulo-6man-rfc3484-update-00 (work in progress), November 2007.

[42] ——, "Default Locator-pair selection algorithm for the SHIM6 protocol." Internet Engineering Task Force, draft-ietf-shim6-locator-pair-selection-02 (work in progress), July 2007.

[43] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture." RFC4423, RFC Editor United States, 2006.

[44] T. Henderson and B. Works, "Host mobility for IP networks: a comparison," *Network, IEEE*, vol. 17, no. 6, pp. 18–26, 2003.

[45] R. Katz, "Adaptation and mobility in wireless information systems," *Communications Magazine, IEEE*, vol. 40, no. 5, pp. 102–114, 2002.

[46] R. Katz and E. Brewer, "The Case for Wireless Overlay Networks," *SPIE Multimedia and Networking Conference*, 1996.

[47] M. Stemm and R. Katz, "Vertical handoffs in wireless overlay networks," *Mobile Networks and Applications*, vol. 3, no. 4, pp. 335–350, 1998.

[48] J. Manner, L. Burness, E. Hepworth, A. Lopez, and E. Mitjana, "Provision of QoS in heterogeneous wireless IP access networks," *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, vol. 2, 2002.

[49] L. DellUomo and E. Scarrone, "An all-IP solution for QoS mobility management and AAA in the 4G mobile networks," *International Symposium on Wireless Personal Multimedia Communications*, vol. 2, pp. 591–595, 2002.

[50] M. Inoue, G. Wu, K. Mahmud, H. Murakami, and M. Hasegawa, "Development of MIRAI System for Heterogeneous Wireless Networks," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 1, pp. 69–73, 2002.

[51] L. Morand and S. Tessier, "Global mobility approach with Mobile IP in" All IP" networks," *Communications, 2002. ICC 2002. IEEE International Conference on*, vol. 4, 2002.

[52] M. Buddhikot, G. Chandranmenon, S. Han, Y. Lee, S. Miller, and L. Salgarelli, "Integration of 802.11 and third-generation wireless data networks," *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, vol. 1, pp. 503–512 vol.1, 30 March-3 April 2003.

[53] M. Ylianttila, M. Pande, J. Makela, and P. Mahonen, "Optimization scheme for mobile users performing vertical handoffsbetween IEEE 802.11 and GPRS/EDGE networks," *Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE*, vol. 6, 2001.

[54] R. Chakravorty and I. Pratt, "Performance Issues with General Packet Radio Service," *Journal of Communications and Networks (JCN)*, vol. 4, no. 2, pp. 266–281, 2002.

[55] J. McNair and Z. Fang, "Vertical handoffs in fourth-generation multinetwork environments," 2004.

[56] S. McCann, W. Groting, A. Pandolfi, and E. Hepworth, "Next Generation Multimode Terminals," 2004.

[57] Q.Zhang, C.Guo, Z.Guo, W., and W.Zhu, "Efficient mobility management for vertical handoff between WWAN and WLAN," 2003.

[58] V. Gupta and D. Johnston, "A Generalized Model for Link Layer Triggers," March 2004. [Online]. Available: www.ieee802.org/handoff/march04_meeting_docs/Generalized_triggers-02.pdf

[59] P. Vidales, C. J. Bernardos, G. Mapp, F. Stajano, and J. Crowcroft, "A Practical Approach for 4G Systems: Deployment of Overlay Networks," pp. 172 – 181, February 2005.

[60] R. Chakravorty, P. Vidales, K. Subramanian, I. Pratt, and J. Crowcroft, "Performance issues with vertical handovers-experiences from GPRS cellular and WLAN hot-spots integration," *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*, pp. 155–164, 2004.

[61] H. Einsiedler, R. Aguiar, J. Jähnert, K. Jonas, M. Liebsch, R. Schmitz, P. Pacyna, J. Gozdecki, Z. Papir, J. Moreno, *et al.*, "The Moby Dick Project: A Mobile Heterogeneous All-IP Architecture," *Int. Conf. Advanced Technologies, Applications and Market Strategies for 3G (ATAMS'01), Cracow, Poland, Jun*, 2001.

[62] A. Cuevas, P. Serrano, C. Bernardos, J. Moreno, J. Jaehnert, K. Hyung-Woo, J. Zhou, D. Gomes, P. Gonçalves, and R. Aguiar, "Field Evaluation of a 4G True-IP network," *IST Mobile Summit 2004*, 2004.

[63] V. Marques, R. Aguiar, C. Garcia, J. Moreno, C. Beaujean, E. Melin, M. Liebsch, and P. Inovacao, "An IP-based QoS architecture for 4G operator scenarios," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 10, no. 3, pp. 54–62, 2003.

[64] "Technical Specification Group RAN: Signalling enhacements for Circuit-Switched (CS) and Packet-Switched (PS) Connections;Analyses and Recommendations(Release 7)." 3GPP.

[65] T. D. P. (first phase), "Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services," 006. [Online]. Available: http://www.ist-daidalos.org/

[66] T. D. P. (second phase), "Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services," 006. [Online]. Available: http://www.ist-daidalos.org/

[67] R. Aguiar, A. Banchs, C. Bernardos, M. Calderon, M. Liebsch, T. Melia, P. Pacyna, S. Sargento, and I. Soto, "Scalable QoS-Aware Mobility for Future Mobile Operators," *in IEEE Communications Magazine, due June*, 2006.

[68] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, T. Kodama, and H. Schulzrinne, "Seamless Handoff across Heterogeneous Networks - An 802.21 Centric Approach," *International Symposium on Wireless Personal Multimedia Communications (WPMC), IEEE*, 2005.

[69] Y. An, B. Yae, K. Lee, Y. Cho, and W. Jung, "Reduction of Handover Latency Using MIH Services in MIPv6," *Proceedings of the International Conference on Advanced Information Networking and Applications*, vol. 2, pp. 229–234, 2006.

[70] P. Magnusson, J. Lundsjo, J. Sachs, and P. Wallentin, "Radio resource management distribution in a beyond 3G multi-radio access architecture," *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, vol. 6.

[71] K. Nishida, S. Isobe, T. Yagyu, and I. Akiyoshi, "Implementation and Evaluation of a Network-Controlled Mobility Management Protocol (IP2MM): Performance Evaluation Compared with Mobile Ipv6," *Wireless Communications and Networking Conference*, vol. 3, pp. 1402–1408, 2005.

[72] J. Zander, "Radio resource management in future wireless networks: requirements and limitations," *Communications Magazine, IEEE*, vol. 35, no. 8, pp. 30–36, 1997.

[73] A. Tolli, P. Hakalin, and H. Holma, "Performance evaluation of common radio resource management (CRRM)," *Communications, 2002. ICC 2002. IEEE International Conference on*, vol. 5, 2002.

[74] A.-E. M. Taha, H. S. Hassanein, and H. T. Mouftah, "On Robust Allocation Policies in Wireless Heterogeneous Networks," *First International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks,IEEE*, pp. 198–205, June 2004.

[75] P. Bertin, K. Guillouard, and J. Rault, "IP based network controlled handover management in WLAN access networks," *Communications, 2004 IEEE International Conference on*, vol. 7, 2004.

[76] D. Kutscher and J. Ott, "Service Maps for Heterogeneous Network Environments; Mobile Data Management," *The 7th International Conference on Mobile Data Management, IEEE*, 2006.

[77] K. YoussefKhouaja, P. Bertin, and J. Botmin, "Hierarchical Mobility Controlled by the Network," *Multiaccess, Mobility and Teletraffic for Wireless Communications*, 2002.

[78] I. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 11, no. 4, pp. 16–28, 2004.

[79] J. Bi, P. Hu, and L. Xie, "Site Multihoming: Practices, Mechanisms and Perspective," *Future Generation Communication and Networking*, vol. 1, 2007.

[80] T. Chen and L. Wenyu, "A Novel IPv6 Communication Framework: Mobile SHIM6 (M-SHIM6)," *Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006. International Conference on*, pp. 1–3, 2006.

[81] M. Bagnulo, A. Garcia-Martinez, and A. Azcorra, "IPv6 multihoming support in the mobile internet," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 14, no. 5, pp. 92–98, 2007.

[82] S. Barré and O. Bonaventure, "Improved Path Exploration in shim6-based Multihoming," *Proc. ACM SIGCOM IPv6 Workshop, Aug*, 2007.

[83] E. Wu, J. Lai, and A. Sekercioglu, "An Accurate Simulation Model for Mobile IPv6 Protocol," *Proceedings of Australian Telecommunications, Networks and Applications Conference ATNAC04*, 2004.

[84] J. Lei, R. Yates, L. Greenstein, and H. Liu, "Wireless Link SNR Mapping Onto An Indoor Testbed," *2nd International IEEE/Create-Net Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (Tridentcom)*, 2005.

[85] S. Zvanovec, M. Valek, and P. Pechac, "Results of indoor propagation measurement campaign for WLAN systems operating in 2.4 GHz ISM band," *Antennas and Propagation, 2003.(ICAP 2003). Twelfth International Conference on (Conf. Publ. No. 491)*, vol. 1.

[86] M. Lott and I. Forkel, "A multi-wall-and-floor model for indoor radio propagation," *Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd*, vol. 1, 2001.

[87] "Universal Mobile Access (UMA) User Perspective (Stage 1) R 1.0.0." Alcatel, AT&T Wireless Services, BT PLC, Cingular Wireless LLC, Ericsson AB, Kineto Wireless Inc, Motorola, Nokia, Nortel Networks, O2, Rogers Wireless, Siemens AG, Sony Ericsson, T-Mobile USA.

[88] "Universal Mobile Access (UMA) Architecture (Stage 2) R 1.0.4." Alcatel, AT&T Wireless Services, BT PLC, Cingular Wireless LLC, Ericsson AB, Kineto Wireless Inc, Motorola, Nokia, Nortel Networks, O2, Rogers Wireless, Siemens AG, Sony Ericsson, T-Mobile USA.

[89] M. Liebsch, A. Singh, H. Chaskar, D. Funato, and D. Funato, "Candidate Access Router Discovery (CARD)." RFC4066, RFC Editor United States, 2005.

[90] D. Lister, S. Dehghan, R. Owen, P. Jones, and U. Vodafone-Airtouch, "UMTS capacity and planning issues," *3G Mobile Communication Technologies, 2000. First International Conference on (IEE Conf. Publ. No. 471)*, pp. 218–223, 2000.

[91] T. Melia, D. Corujo, A. de la Oliva, A. Vidal, R. Aguiar, and I. Soto, "Impact of heterogeneous network controlled handovers on multi-mode mobile device design," *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 3884–3889, 2007.

[92] [Online]. Available: http://enjambre.it.uc3m.es/~aoliva/reap.html

[93] D. Katz and D. Ward, "Bidirectional Forwarding Detection." Internet Engineering Task Force, draft-ietf-bfd-base-07 (work in progress), January 2008.

[94] A. de la Oliva, T. Melia, A. Banchs, I. Soto, and A. Vidal, "IEEE 802.21 (Media Independent Handover Services) Overview," *Accepted for publication in Wireless Communication Magazine, IEEE*.

[95] A. de la Oliva, T. Melia, A. Vidal, C. J. Bernardos, I. Soto, and A. Banchs, "A case study: IEEE 802.21 enabled mobile terminals for optimised WLAN/3G handovers," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, April 2007.

[96] T. Melia, A. de la Oliva, I. Soto, C. J. Bernardos, and A. Vidal, "Analysis of the effect of mobile terminal speed on WLAN/3G vertical handovers," *2006 IEEE Global Telecommunications Conference (GLOBECOM)*, December 2006.

[97] T. Melia, A. de la Oliva, I. Soto, P. Serrano, and R. Aguiar, "Network Controlled Handovers: challenges and possiblities," *Wireless Personal Communications Journal*, vol. 43, November 2007.

[98] T. Melia, A. de la Oliva, A. Vidal, I. Soto, D. Corujo, and R. Aguiar, "Toward IP Converged Heterogeneous Mobility: A Network Controlled Approach," *Computer Networks*, vol. 51, pp. 4849–4866, December 2007.

[99] A. de la Oliva, I. Soto, A. García-Martínez, M. Bagnulo, and A. Azcorra, "Analytical Characterization of Failure Recovery in REAP," *Submitted to IEEE/ACM Transactions on Networking*.

[100] A. de la Oliva, M. Bagnulo, A. Garcia-Martinez, and I. Soto, "Performance Analysis of the REAchability Protocol for IPv6 Multihoming," *NEW2AN 2007, Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking*, September 2007.

[101] T. Melia, D. Corujo, A. de la Oliva, A. Vidal, R. Aguiar, and I. Soto, "Impact of heterogeneous network controlled handovers on multi-mode mobile device design," *IEEE Wireless Communications and Networking Conference 2007 - Networking (WCNC2007)*, 2007.

[102] T. Melia, L. Boscolo, A. Vidal, A. de la Oliva, and M. Zorzi, "IEEE 802.21 reliable event service support for network controlled handover scenarios," *2007 IEEE Global Telecommunications Conference (GLOBECOM)*, 2007.

[103] A. Sanmateu, L. Morand, E. Bustos, S. Tessier, F. Paint, and A. Sollund, "Using mobile IP for provision of seamless handoff between heterogeneous access networks, or how a network can support the always-on concept. EURESCOM Summit, 2001."

[104] "IEEE 802.11 Wireless Local Area Network." [Online]. Available: http://www.ieee802.org/11/

[105] M. WILLIAMS, "Directions in Media Independent Handover," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, pp. 1772–1776, 2005.

[106] O. S. Y. et al., "A Handover Framework for Seamless Service Support between Wired and Wireless Networks," *Advanced Communication Technology (ICACT) 2006, vol. 3 20-22, p1791-1796*, February 2006.

[107] J. Lai, E. Wu, A. Varga, Y. Sekercioglu, and G. Egan, "A Simulation Suite for Accurate Modeling of IPv6 Protocols," *Proceedings of the 2nd International OMNeT++ Workshop*, pp. 2–22, 2002.

[108] S. Woon, E. Wu, and A. Sekercioglu, "A Simulation Model of IEEE802. 11b for Performance Analysis of Wireless LAN Protocols," *Australian Telecommunications, Networks and Applications Conference (ATNAC)*.

Acronyms

3G *Third Generation*

3GPP *3rd Generation Partnership Project*

3GPP2 *3rd Generation Partnership Project 2*

4G *Fourth Generation*

ADSL *Asymmetric Digital Subscriber Line*

AP *Access Point*

AS *Autonomous System*

ASN *Autonomous System Number*

BACK *Binding Acknowledgement*

BFD *Bidirectional Forwarding Detection*

BGP *Border Gateway Protocol*

BID *Binding Unique Identification*

BSS *Base Station*

BU *Binding Update*

CN *Correspondent Node*

CoA *Care-of Address*

CoT *Care-of Test*

CoTI *Care-of Test Init*

CS *Command Services*

DAD *Duplicate Address Detection*

DHCP *Dynamic Host Configuration Protocol*

DNS *Domain Name System*

DoS *Denial of Service*

ES *Event services*

FMIP *Fast Handovers for Mobile IPv6*

FTP *File Transfer Protocol*

GPRS *General Packet Radio Service*

GPS *Global Positioning System*

GSM *Global System for Mobile communications (GSM: originally from Groupe Special Mobile)*

HA *Home Agent*

HMIP *Hierarchical Mobile IPv6*

HoA *Home Address*

HoT *Home Test*

HoTI *Home Test Init*

ID *Identificator*

IE *Information Element*

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*

IS *Information Services*

ISP *Internet Service Provider*

L2 *Layer two (MAC layer)*

L3 *Layer 3 (IP Layer)*

LAN *Local Area Network*

LTE *Long Term Evolution*

MAC *Medium Access Control*

MICS *Media Independent Command Service*

MIES *Media Independent Event Service*

MIH *Media Independant Handover*

MIHF *Media Independant Handover Function*

MIHO *Mobile Initiated Handovers*

MIIS *Media Independent Information Service*

MIPv6 *Mobile IPv6*

MN *Mobile Node*

NCHO *Network Controlled Handovers*

NETLMM *Network based Localized Mobility management*

NIHO *Network Initiated Handovers*

NUD *Neighbor Unreachability Detection*

P2P *Peer to Peer*

PDP *Packet Data Protocol*

PDU *Protocol Data Unit*

PHY *Physical Layer*

PoA *Point of Attachment*

PoS *Point of Service*

PPP *Point to Point Protocol*

QoS *Quality of Service*

REAP *REAchability Protocol*

RFC *Request for Comments*

RSSI *Received Signal Strength Indicator*

RTT *Round Trip Time*

SAP *Service Access Point*

SCTP *Stream Control Transmission Protocol*

SHIM6 *Site Multihoming by IPv6 Intermediation*

SIP *Session Initiation Protocol*

SS *Single Sample*

TCP *Transport Control Protocol*

TD-CDMA *Time Division-Code Division Multiple Access*

TLV *Type, Length, Value*

UDP *User Datagram Protocol*

UL *Upper Layers*

ULID *Upper Layers Identifier*

UMTS *Universal Mobile Telecommunications System*

VoIP *Voice over IP*

WG *Working Group*

WiFi *Wireless Fidelity*

WiMAX *Worldwide Interoperability for Microwave Access*

WLAN *Wireless Local Area Network*

WM *Weighted mean*

WM3S *Weighted mean of three samples*

WMPM *Weighted mean with the previous mean*