Faculdade de Engenharia da Universidade do Porto

Implementation of the IEEE 802.21 in the Network Simulator 3

Adriano Tavares da Silva Pinho

Thesis submitted under the
Integrated Master Degree in Electrical and Computer Engineering
Major Telecommunications

Supervisor: Prof. Dr. Manuel Alberto Pereira Ricardo
Co-Supervisor: Eng. Gustavo João Alves Marques Carneiro

June 2008

U.PORTO
FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES 2007/2008

A Dissertação intitulada

"Implementation of the IEEE 802.21 in the NS3 Simulator"

foi aprovada em provas realizadas 18/Julho/2008

o júri

Presidente Professor Doutor Mário Jorge Moreira Leitão
Professor Associado da Faculdade de Engenharia da Universidade do Porto

Professora Doutora Susana Isabel Barreto de Miranda Sargento
Professora Auxiliar Convidada da Universidade de Aveiro

Professor Doutor Manuel Alberto Pereira Ricardo
Professor Associado da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projecto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são correctamente citados.

Autor - Adriano Tavares da Silva Pinho

Faculdade de Engenharia da Universidade do Porto

Abstract

Today's networks prime for mobility. A Mobile which is connected to a specific Access Point may be transferred from one Access Point to another, even during a call. This transfer is called a Handover. UMTS and GSM use this concept every day, when a user is performing a call and moves from one location to another, switching the Access Point to which the Mobile Device is connected. However, this handover is made within the access technology.

True mobility does not restrain itself to a specific access technology, which is why there is an effort to create a handover that works between them. The IEEE 802.21 uses network devices like the ones used in UMTS and Wifi to perform a handover. The Media Independent Handover Function (MIHF) is used by IEEE 802.21, to provide events, controls and even information for an application to use. The Media Independent Information Service (MIIS) can be thought of as complement to the MIHF, using the services and commands provided to implement the handover. It also uses a SPARQL to query a RDF Server for information related to the Access Points in the vicinity, thought the MIHF. The DHCP is used by the MIIS, due to the MIIS's implementation as a mobility agent.

In this work an implementation of an IEEE 802.21 framework was made, demonstrating its advantages in the handover process. A handover scenario using the framework presented demonstrates the seamless handover with the MIHF, in opposition with the handover without the MIHF. The main difference between this two handover times is the information provided by the MIIS, which in the handover scenario, determines the need for a Wifi channel scan.

Acknowledgements

A very special thanks to everyone who has provided support and motivation in the course of my work, especially Eng. Gustavo Carneiro who has always extended time and provided encouragement in the work developed. I would also like to thank Dr. Manuel Ricardo for the motivation provided. As for my family and friends, thanks for all the support. My best wishes to everyone for their future.

Table of Contents

List of Figures

List of Tables

List of Excerpts

Abbreviations and Acronyms

4G	Forth Generation
AP	Access Point
AuC	Authentication Center
BS	Base Station
BSC	Base Station Controller
BSS	Basic Service Set
BTS	Base Station Transceiver
BWA	Broadband Wireless Access
CN	Correspondent Node
CoA	Care of Address
DEEC	Departamento de Engenharia Electrotécnica e de Computadores
DHCP	Dynamic Host Configuration Protocol
DS	Distribution System
DSS	Distribution System Service
EIR	Equipment Identity Register
ESS	Extended Service Set
FA	Foreign Agent
FBSS	Fast BS Switching
FEUP	Faculdade de Engenharia da Universidade do Porto
FT	Fast Transition
GMSC	Gateway MSC
GSM	Global System for Mobile communications
HLR	Home Location Register
ICMP	Internet Control Message Protocol
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
L2	Layer 2
L3	Layer 3
MDHO	Macro Density Handover
MIC	Message Integrity Check
MIH	Media Independent Handover
MIHF	Media Independent Handover Function

MIP	Mobile IP
MN	Mobile Node
MS	Mobile Station
MSC	Mobile Switching Center
NFA	Next Foreign Agent
NS3	Network Simulator 3
OSI	Open Systems Intercommunication
PFA	Previous Foreign Agent
PMK	Pairwise Master Keys
PoA	Point of Access
PoS	Point of Service
PTK	Pairwise Temporal Keys
QoS	Quality of Service
RA	Router Advertisement
RDF	Resource Description Framework
RNC	Radio Network Controller
SQPARL	SPARQL query language
SS	Station Service / Subscriber Stations
STA	Station
TLV	Type – Length - Value
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
VLR	Visitor Location Register
XML	Extensible Markup Language

Chapter 1

Introduction

In today's networks, a user with a mobile can easily perform a call though a GSM link. This link involves not only the two mobile phones, but also a Point of Access (PoA), some network devices and information that travels between the network and the mobile phone, in order to connect the two users that are using the call. Assuming that one of the users in the call is moving, this user will continue to use the same connection via the same point of access (PoA) as before, while he remains in the range area of the PoA. However, if he leaves the range area of the PoA, the mobile will try to connect to another PoA. If this is successful, the cellular mobile will connect via the new PoA without the user even acknowledges it. This is called a horizontal handover.

In the future, 4G communications [1] will allow communications to use all types of services based on IP, and perform a soft handover between heterogeneous networks. Today, the 802 standards do not support handover between different types of networks, and do not provide triggers or other services to accelerate handovers based on mobile IP. However, these standards provide mechanisms to detect and select network access points, but do not allow detection and selection independently of the type of network.

The objective of the work described here is twofold. On one hand, a framework for simulation of 802.21 based network scenarios in NS-3 is meant to be provided. On the other hand, to demonstrate the advantages of 802.21 in general, and the simulation framework that was developed, by studying how 802.21 can substantially improve handover times is also important.

In this document, the reader will be able to check the State of the Art, in which it will be possible to see what was be used to implement the work at hand, such as the Semantic Web, used by the MIIS to retrieve information. After that, there will be a chapter describing IEEE 802.21. The Network Simulator 3 and the framework developed for the simulation of the IEEE 802.21 are also referred, followed by a study of a handover scenario and the final conclusions of the project.

Chapter 2

State Of The Art

This chapter introduces future references that will be used afterwards. Some Mobile Devices are described, such as the IP Connectivity procedures to create a successful handover, after a link is disconnected. The Semantic Web is also referred, since it is used by 802.21 as an information system to store and retrieve information from the server, concerning the neighboring PoAs.

2.1 Mobile Networks

The IEEE 802.11, the IEEE 802.16 and the UMTS are described in this chapter. As the reader may confirm, there are also some amendments that refer to the handover between a Station and two Points of Service, which use the same access Technology.

2.1.1 802.11

The 802.11 networks, or Wi-Fi, are known for their success in providing network access, completely wireless. Today, they are the standard wireless access to hotspots all over the world.

The architecture behind an 802.11 network, as seen in Figure 2.1, consists in a station (STA) [5], which is the device that accesses the network. This device can be at a fixed position, or it can be mobile, thus having the possibility to execute handover. A Basic Service Set (BSS) provides a coverage area for STAs to connect to a specific Access Point, which are interconnected by a Distribution System (DS). The DS can be a wired or a wireless network. The Access Points (AP), are used to connect the DS to the BSS, whereas the Portal connects the 802.11 network with another non 802.11 network. The Extended Service Set (ESS) is defined as a group of DS and BSS with some complexity. Finally, there are two services associated with the two major components of the 802.11 service. They are the Station Service (SS), and the Distribution System Service (DSS).

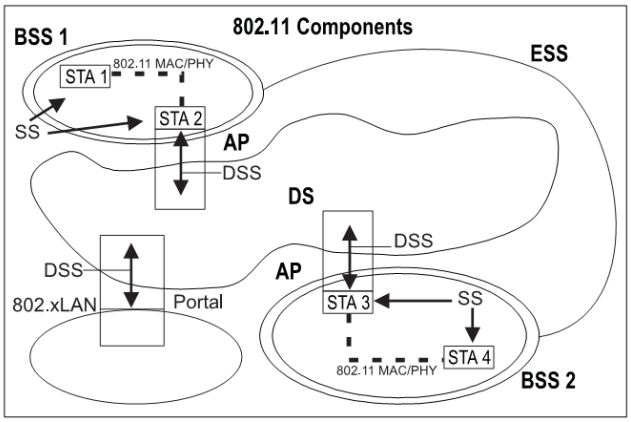

Figure 2.1 - IEEE 802.11 Network Elements

2.1.1.1 Wifi Scanning

The scanning for an AP by a Station, comprises one of two connection methods [6]. In passive scanning, the Station waits for a Beacon Frame sent by an AP, for each channel to scan. It normally waits until the beacon interval expires, which is about 100 ms, to change the channel which is scanning.

(2.1) $$ScanningTime = BeaconInterval * NumberOfChannels$$

When a Station actively searches the medium, by sending Probe Request Frames and waiting for Probe Response frames, it is performing active scanning. The active scanning also enterprises a timeout, of about 50 ms, needed in order to discover that no AP is using a channel. Since both the scanning procedures depend on the number of channels and on the timeout of the method chosen, one may assume that the Active Scanning takes half the time of the Passive Scanning.

(2.2) $$ScanningTime = ActiveScanningTimeout * NumberOfChannels$$

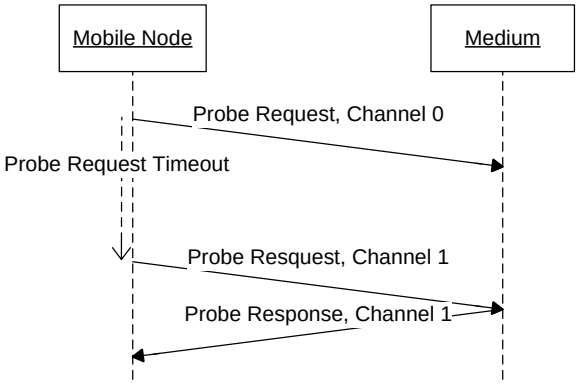

Figure 2.2 – Active Scanning

2.1.1.2 Wifi States

When a Station finds an AP, it goes though two major processes to connect or disconnect to the network. The Authentication process, whereas a Station authenticates to an AP, and interchange information. An example of an information relevant is the acknowledgment of a given password. The Association process, described by the information exchanged, includes the stations and the BSS capabilities. Only after the Association process, a station is capable of transmitting and receiving data frames. The process by which a Station connects to the network, can be summarized in Figure 2.3. We can distinguish three main stages, each of them describing the process by which a station connects or disconnects to a network, using the Association process and the Authentication process.

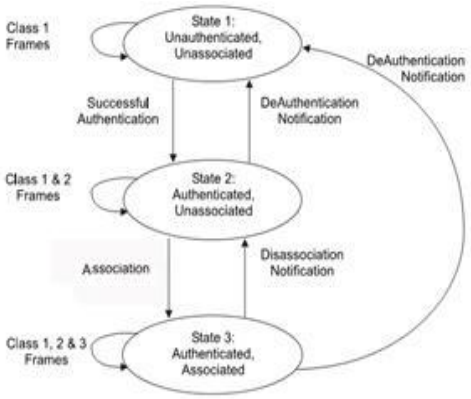

Figure 2.3 - States involved in the 802.11 network processes

2.1.1.3 Handover

In an 802.11 network, a handover, or transition between the connection of a station to a previous AP, and the connection of a station to a new AP, comprises two major phases. The scanning phase, is characterized by the discovery of a new station to connect to. In this phase, as previously described, the station can either scan the medium passively, or actively. In the re-association phase, one may observe the authentication and association processes already described. After this phase, the station is ready to receive and send data packets.

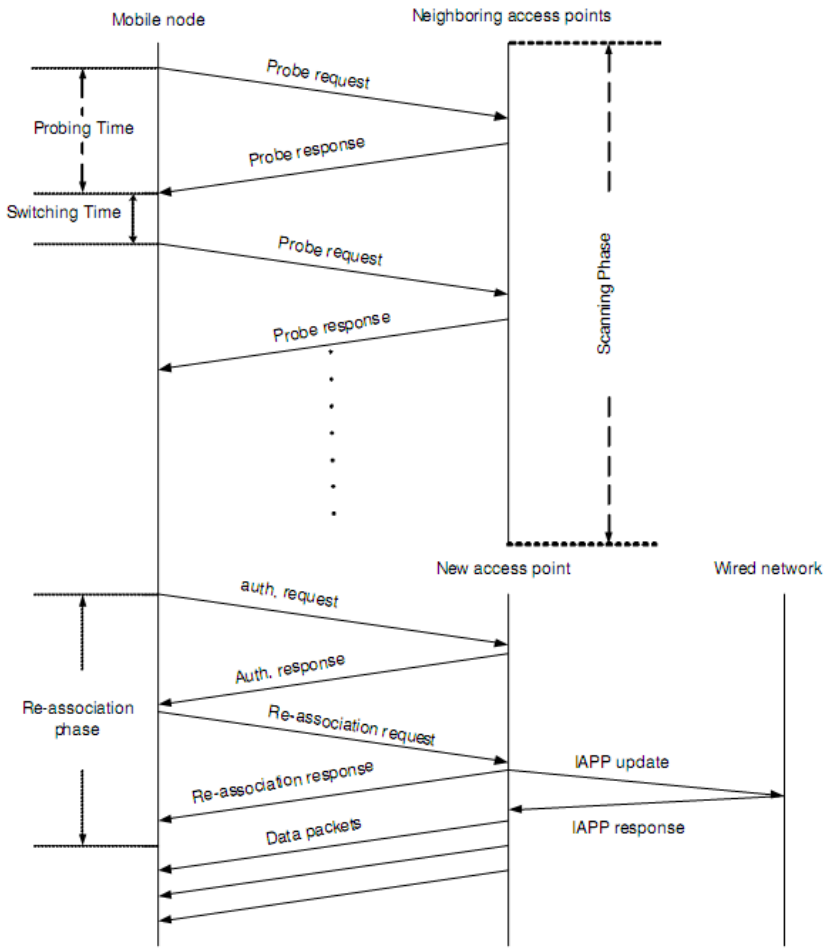

Figure 2.4 - Handover procedure

2.1.1.4 802.11r

This amendment to the 802.11 describes methods in order to minimize the amount of time the data connectivity is lost due to a transition between a Station and a BSS. As can be seen from Figure 2.5, the BSS transition process, in which the Mobile Node (STA) roams from one access point (AP) to another, may consist in 6 stages [9]:

1. Discovery, or Probe exchange,
2. 802.11 open authentication,
3. Re-association,
4. Authentication method,
5. EAPOL key exchange,
6. QoS negotiation.

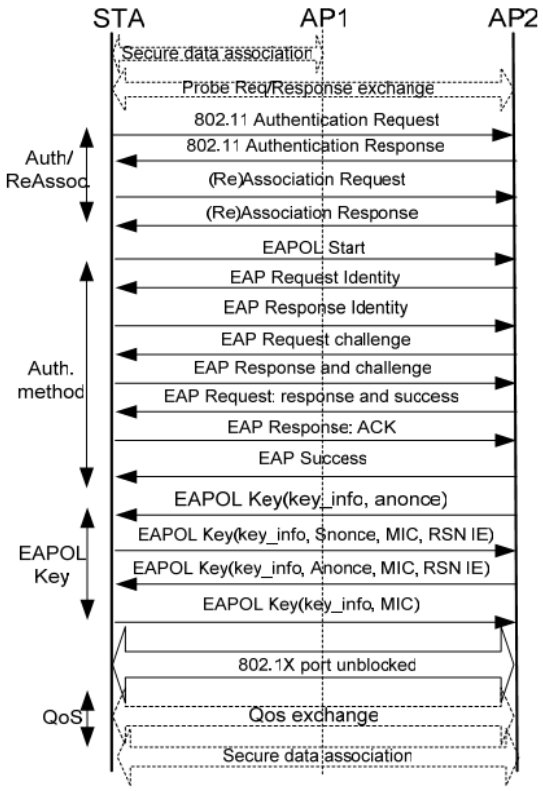

Figure 2.5 - Authentication and QoS exchange process during transition

The authentication process involves the mobile, the AP and the authentication server. In this process, the mobile sends authentication requests to the AP, and the authentication server checks the credentials of the mobile and authorizes it. The authorization involves a response from the server to the AP and the mobile. After the first authentication messages, the server and the mobile agree on a PMK (Pairwise Master Key), which is distributed to the AP. After they authenticate, they derive a set of PTK (Pairwise Temporal Keys) for encryption purposes and then perform an EAPOL 4-way handshake to establish the keys.

Analyzing the authentication process described, we can observe a process that may take a few hundreds of milliseconds. This time is far too large and results in "hiccups" during a voice conversation between mobiles. The recommended method for the PMK generation is that it should be done when the mobile joins the network, and then distributed to all AP's. This is one of the important implementations in order to reduce the time taken in roaming. The other improvements involve the 4-way handshake and the traffic specification negotiation, which are performed and completed during the re-association.

2.1.1.5 QoS Features

In 802.11r [9], the station may request QoS (Quality of Service) at the time of re-association, thus saving time in performing roaming, and preserving voice quality. However, in some cases the re-association time may take longer than desired, in which case the mobile takes benefits from being able to reserve resources prior to re-associating. As an example of these cases, if the AP is heavily loaded, the mobile may reserve resources before it re-associates.

2.1.1.6 Transition Mechanisms

After the mobile makes initial contact, and informs the AP that it plans to use the Fast Transition (FT) when it roams to other APs, the mobile determines an AP to associate by examining beacon and/or probe responses for Information Elements (IE), which represents information. This information may be obtained by 802.11k, or be provided by 802.21. When the AP is determined, the mobile performs an 802.11 open authentication, and sends an association request containing the IEs. The association request indicates the FT mechanisms it wishes to use. The authentication mechanism takes care of determining the keys used.

Once the mobile has performed the first contact successfully, it may execute the FT mechanisms in the transition. The PTK set-up and the QoS resources allocation may be performed before, or at, re-association.

The base mechanism accomplishes transition in two stages [9]. The first stage establishes the information needed for the PTK, and the second stage executes the re-association. In this re-association stage, the mobile requests any resource allocated needed, and includes a Message Integrity Check (MIC) to authenticate the request. The AP's response contains a response to the resource request, the group temporal key and any associated key index, as well as the MIC.

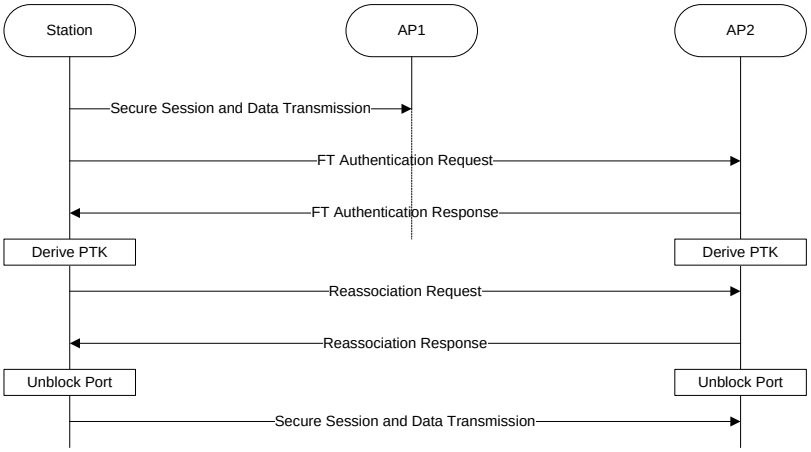

Figure 2.6 - Base Transition

The AP's may support the reservation mechanisms for fast transitions. Fast Transition with reservation is accomplished in three stages. The first stage is maintained as the first stage of the base mechanism already referred. The second stage allows resource reservation. The mobile sends its resource requirements to the target AP, and includes the MIC calculated. The AP's response includes details about the resource reservation, and contains MIC to validate the response. The third stage is the re-association stage, as seen previously in the base mechanism. During the fast transition, the mobile may authenticate and reserve resources from one or more APs, choosing then which AP to connect to.

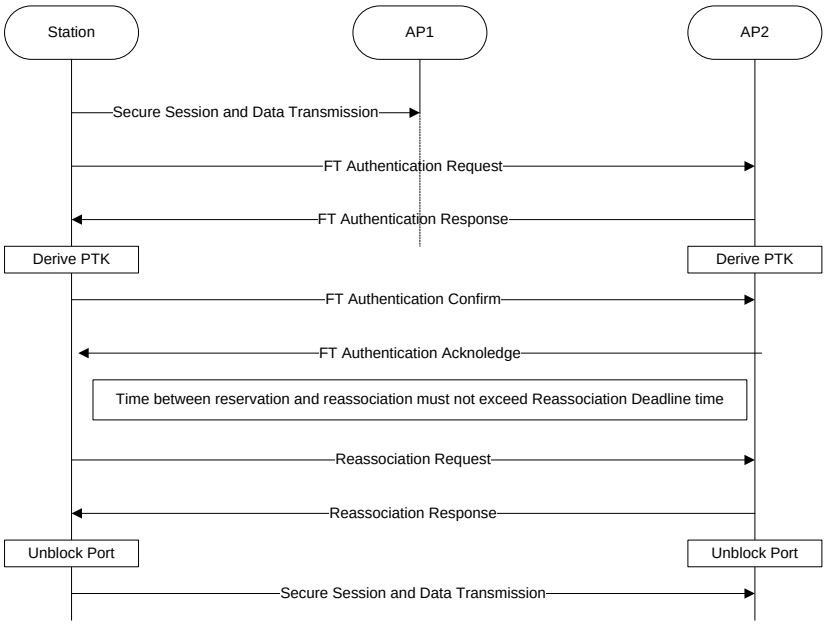

Figure 2.7 - Transition with Reservation

2.1.2 802.16

The 802.16 is the referred protocol behind the Broadband Wireless Access (BWA). It supports a primarily point to point architecture, with an optional mesh topology. There are two types of topologies, the PMP and the mesh mode [10].

In the PMP mode, the wireless link operates with a central Base Station (BS) and an antenna, capable of handling multiple sectors simultaneously. Normally, the transmissions sent by the BS in the downlink are broadcast. The uplink is shared by the Subscriber Stations (SS); however, the SS may be issued continued rights to transmit. These rights may be granted by the BS after the request by a user.

In the Mesh mode, the traffic occurs not only between the BS and the SS, but it may also occur through SS and directly between SS. In this topology, the Mesh BS cannot transmit before it coordinates its transmissions with the BS within the two-hop neighborhood. This ensures the quality of the transmission and avoids collisions. QoS in this topology is provided on a message by message basis.

The overall steps in the network entry may be described as follows:

1. Scan for downlink channel and synchronization, where the SS will first try to connect to the last connected channel available. If this fails, then the SS will scan the network until it finds a valid signal.
2. Obtain parameters, for the downlink and the uplink;
3. Perform ranging, where the SS acquires the correct timing offset and power adjustments;
4. Negotiate Basic capabilities;
5. Authorize SS and perform key exchange;
6. Perform registration, with the BS;
7. Set up connections.

2.1.2.1 Handover in 802.16e

IEEE 802.16e is an amendment to IEEE 802.16 for mobile operations. It has three optional Handover procedures. The first, the Hard Handover, is the base operation method. The Macro Diversity Handover (MDHO) and Fast BS Switching (FBSS) are optional, and may not be present in an implemented 802.16 network.

The Hard Handover process present in 802.16e [11] may be observed in Figure 2.8. The steps involved may be summarized in the four steps. Cell reselection is defined by the use of the information acquired from a Neighbor BS to perform or schedule scanning intervals. HO Initiation and Decision, may be decided by the MS or the BS, whereas Synchronization with the new downlink may be described as a synchronization of resources between the MN and the BS. Finally, the final step is Ranging, which may be faster or slower, depending on the amount of information possessed by the Mobile Node, relatively to the new BS.

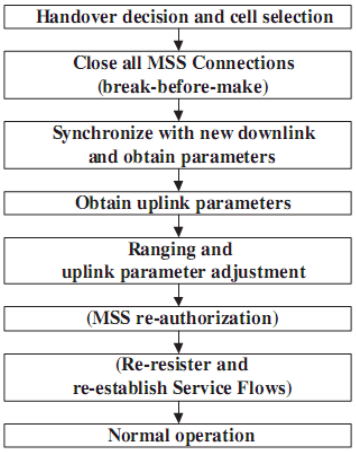

Figure 2.8 - Handover

With both the MDHO and the FBSS, the Handover procedure has three stages:

1. Handover Decision. In MDHO, the step begins with the decision to transmit and receive from multiple BS at the same time. In FBSS, the handover is started with the decision to receive and transmit data to an Anchor BS.
2. Diversity Set Selection/Update, where the MN scans the neighbor BS and select the ones to include in the diversity set.
3. Anchor BS Selection/Update, whereas the MN monitors the signal strength of the BS in the Diversity Set, and selects one BS to be the Anchor BS.

2.1.3 UMTS

The Universal Mobile Telecommunication System (UMTS) is the standard behind the 3G networks. The comparison with the 2G provides improvements, like wider bandwidth and chip rate [12], provision of multirate services, complex Spreading, coherent uplink, additional pilot channel in the downlink, seamless interference handover and fast power control in the downlink. The UMTS also provides different QoS parameters for quality of service, which depend on the type of traffic. It supports user features such as Internet Access, Intranet/Extranet Access, Customized information/Entertainment, Multimedia Messaging and Location-Based Services.

The UMTS network, as can be seen in Figure 2.9, uses some of the GPRS network elements. It consists in a User Equipment (UE), or Mobile Station (MS), a Base Transceiver Station (BTS), a Base Station Controller, a Visitor Location Register (VLR), a Home Location Register (HLR), a Mobile Switching Center (MSC), an Authentication Center (AuC), a Gateway MSC (GMSC), an Equipment Identity Register (EIR) and a Radio Network Controller (RNC). A BTS includes the radio equipment used for a user to make a connection, whereas the BSC controls and manages the BTS. A MSC provides connection to other MSC and BSC, and the GMSC provides access to the public telephone network. The VLR and HLR both stores

information, but the first stores it temporary and is related to the Mobile Node currently in the network. The HLR stores information for all users in the network. The AuC contains the algorithms for authenticating subscribers and keys for encryption. The EIR stores identities of all the Mobile Stations in the Network and the RNC performs functions equivalent to the BSC functions in the GSM.

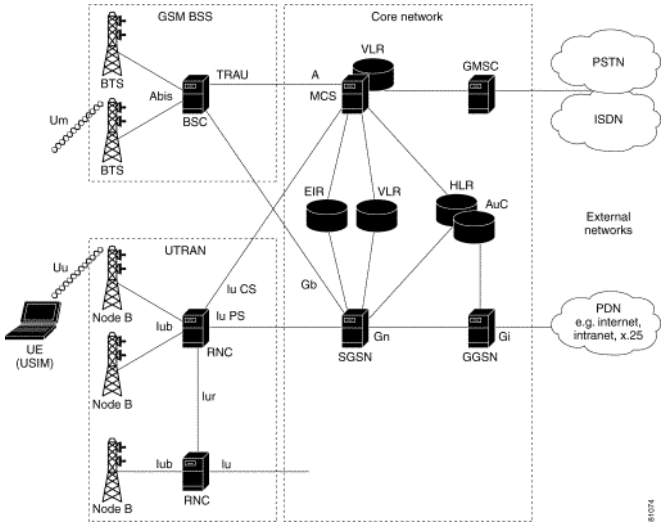

Figure 2.9 - UMTS network

2.1.3.1 Handover

In UMTS, handovers are seamless, due to the fact that the handover is not perceptible to the user and its capability of performing a search on a carrier frequency without affecting the normal data flow. The process behind a handover in UMTS consists in the following stages [13]:

1. Measurement, analysis and initiation;
2. Selection of the controlling entity, BSC or MSC;
3. New link setup via the new point of attachment;
4. Old to new attachment via a switch or bridge;
5. Instructing mobile terminal to switch, case the handover is started remotely;
6. Release of old resources.

2.2 IP Connectivity

In order to establish a connection between the Mobile Node and a Point of Access between a handover, a MAC Level connection is not enough. The IP Level connection may need to be redefined to include, for instance, the Point of Access as the default route of the Mobile Node. In this Chapter, there is a brief characterization of the Mobile IP and the DHCP.

2.2.1 Mobile IP

In order for a mobile device to be truly mobile [3], the routing for the mobile has to be dynamic, i.e., it cannot send the datagrams to the same place, always. On the other hand, if the datagrams are sent to different locations, the mobile cannot be properly identified by other internet computers. To solve this dilemma, the Mobile IP (MIP) allows mobile nodes to use two different IPs: one for routing and one for identification.

Mobile IP uses four main processes in its operation method. Agent Discovery consists in the discovery of the Mobility Agents and attribution of a Care Of Address. Registration is performed after receiving the Care Of Address. In the Communication and Datagram Delivery the datagrams are sent to the Mobile Node's home address, captured by the Home Agent and tunneled to the Care of Address. The datagrams sent by the Mobile Node will take the standard IP routing mechanisms. The Deregistration is made by registering with the same parameters and lifetime set to 0. This should only occur when the mobile node leaves the foreign network and returns to the home network.

2.2.1.1 Discovery Mechanism

Mobile Nodes become aware of mobility agents in visited and home networks by listening to agent advertisement messages [3]. These messages are an adaptation of the ICMP router Advertisement Protocol, which include periodic broadcasts. Via these messages, a mobile node may determine if it is located at a visited network or at a home network. Alternatively, the Mobile Node may not wait for the periodic broadcasts, in which case, it sends an Agent Solicitation Message. Before the end of this process, a FA assigns a CoA to the Mobile Node.

2.2.1.2 Registration

The registration process guarantees that the home agent will capture and reroute the packets sent to the mobile node, by recording the Care of Address of the Mobile Node. There are two distinct registration procedures [4]. The first, registration directly with the home agent, is performed when the mobile node returns to its home network, or when it is using a co-located CoA. The registration with the home agent via the foreign agent is made if the mobile node is using a foreign agent's CoA.

Both registration procedures use register messages which are enclosed by the IP and UDP headers. However, the registration is different in the two cases. Registration with the home agent via the foreign agent consists of four messages:

1. Registration Request, sent by the Mobile Node to the Foreign Agent to begin the registration process;
2. After the processing of the message, the Foreign Agent sends the Registration Request to the Home Agent
3. The Home Agent sends a Registration Reply for the Foreign Agent denying or accepting the registration,
4. The Foreign Agent processes the message and relays it to the Mobile Node.

The direct registration with the home agent uses only two messages, the Registration Request and the Registration Reply, both sent between the Mobile Node and the Home Agent.

The registration requires a process to protect the home agent from fraudulent users. This process involves the use of an unforgettable value that is sent along with the registration message, and changes with every new registration. The value may be a timestamp or a generated random field, and is inserted into the identification field.

2.2.1.3 Datagram Delivery

The datagram delivery involves a tunnel between the Home Agent and the Mobile Node [3]. Although this tunnel can be made of several encapsulation algorithms, the default algorithm is a simple IP-within-IP encapsulation. The Care Of Address is, in this case, the new IP header, and the encapsulation is identified by the value 4 in the outer field protocol. As for the previous header, only its TTL is decremented by one. There is a minimum encapsulation format. Its presence is defined by the protocol number 55 in the encapsulation protocol, and its length may vary from 8 to 12 bytes.

2.2.1.4 Routing and Handover

Considering an optimization in the delivery of datagrams for the Mobile Node, we may consider that the Home Agent provides an updated binding. In this consideration, a Correspondent Node (CN) checks its binding cache and sends the packet to the Home Agent. Only the first datagram will be sent to the Mobile Node (MN) via the Home Agent (HA). When the message passes through the Home Agent, it will cause the Home Agent to send a binding update to the CN. Then, the CN sends packets directly to the MN.

When the mobility of the Mobile Node causes a transition in the Foreign Agent used, the Mobile Node first registers with the new Foreign Agent (NFA). When this happens, it notifies the previous Foreign Agent (PFA) that it maintains a mobility binding for it, via the new Foreign Agent. The new Foreign Agent, after registration and receiving the notification, sends a Binding Update Message to the previous Foreign Agent, which responds with an Acknowledgement and transmits the packets received to the new Foreign Agent. If the previous Foreign Agent receives a packet, it sends a Binding Warning Message to the Home Agent, which in turn sends a Binding Update Message to the CN. In this way, after the handover of the Mobile Node, the communication resumes as previously.

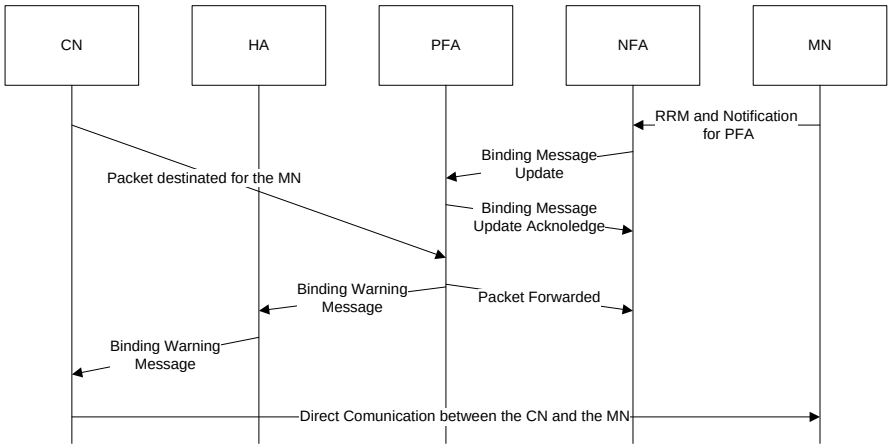

Figure 2.10 - MIP Handover process

2.2.2 DHCP

In a large network, the use of static IP to define values such as the IP Address or the Subnet Mask is, in the least, inefficient. The process by which a Server defines and provides parameters for a new machine that appears in a network is defined as the Dynamic Host Configuration Protocol. It manages and handles the distribution of an IP architecture [28], through a central server or servers. It is also flexible enough to support network segments used by mobile devices [29], i.e., a mobile node that as just been connected to a network may receive dynamically the DHCP parameters.

In the DHCP process, the client starts to broadcast the DHCP DISCOVER message to the local network[30]. The server then captures the message and responds with a DHCP OFFER message, which contains the available address. If the client receives more than one offer, it chooses a server and responds with a DHCP REQUEST message, confirming the address and the server chosen. When the server receives this message, it then responds with a DHCP ACK, containing the configuration parameters, or responds with a DHCP NAK message, if the server could not confirm the DHCP REQUEST received. In any case, if the client cannot use the network, it sends a DHCP RELEASE message, returning the address to the server.

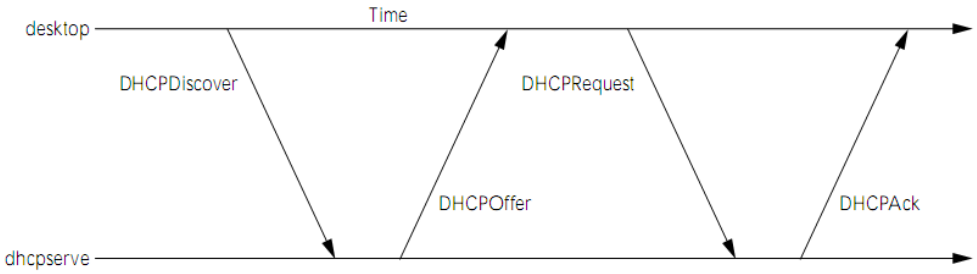

Figure 2.11 - Message Exchange between DHCP Server and DHCP Client

When a DHCP client loses connectivity, due to a reboot of a loss of power, one of three scenarios may occur. For first scenario, the DHCP lease time for the client address is still valid, and the client extends it with the server. In case this lease time is not valid, the client then requests for new DHCP parameters. The same revalidation process may occur if a Mobile Node is transferred from a network access to another, in which case the Mobile Node requests to use an old address and is denied. Finally, if there is a general power failure in the building and the DHCP server is offline at the time the DHCP client starts, the client may use the old address, thus maintaining the general IP structure before the power failure.

2.3 Semantic Web

Semantic Web was initially thought of a structure of information, which may be accessible from both humans and computers. It defines and links information in order to overcome the limitations of the World Wide Web [31], such as lack of structure in information, the ambiguity of web content and the inadequacy for automation information transfers. The advantages of its use, include better communication between platform-independent software agents, the capability to carry automatically sophisticated tasks, and even a way to enable semantic annotations that could be easily found and organized.

The organization in Semantic Web can be thought in RDF, which may be described as a XML-based language that uses a triple based assertion model, consisted in subject – predicate – object, and a syntax to describe resources. The resource may be a web site, a web page, or an object which is named by URIs. The information in a RDF model is structured in triples due to the possibility of description in terms of a subject, an object and a predicate. As for the RDF Schema, it is a model which defines vocabulary for RDF documents, in a specific domain, and by hierarchies [35]. It also defines classes, properties for classes and data types. The structure of and RDF Schema may even be represented by a graph, consisted of nodes, connections and properties.

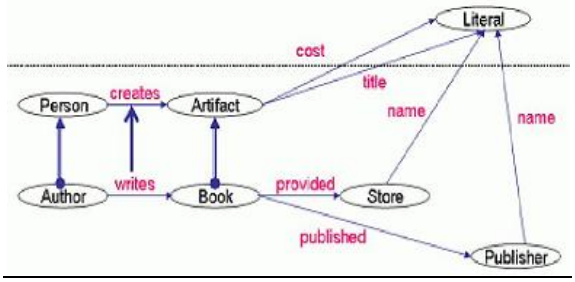

Figure 2.12 - RDF Model [35]

In order to extract information from a RDF model, a query language such as SPARQL query language may be used. The initial efforts at defining semantics and algebraic operations for RDF query language include a navigational model defined on node sets [33], a model based on application of relational algebra, and a definition stated from the perspective of mathematical logic and describing only basic graph paths. Its use normally involves a SPARQL query processor, which analyses the RDF data inserted, that may be a file or web page. After the SPARQL query, the query processor may return its results as XML, or on another format, depending on the processor itself.

Chapter 3

802.21

As can be seen previously, IEEE 802.11r and IEEE 802.16e focus on handovers between the same access technologies, or horizontal handovers. In contrast, IEEE 802.21 is intended to provide methods and procedures that facilitate vertical handover. These handover procedures may use the information gathered from the mobile terminal and the network, in order to satisfy the user requirements and to improve network connections. There are several factors that may determine the handover, such as quality of service, network discovery and power management, but it can be referred that any handover should be done minimizing any perceptible interruption to the user.

The 802.21's framework [2] facilitates the network discovery and selection processes, by exchanging network information that helps mobile devices to determine which networks are in their current neighborhoods. The information may include, for instance, the link type and link identifier of nearby network links. This process of network discovery and selection allows the mobile to connect to the appropriate network.

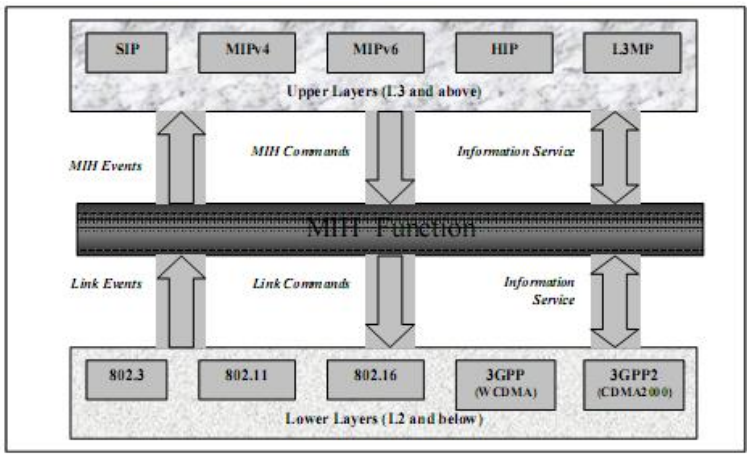

Figure 3.1 - Interaction between MIH components

The core of the 802.21 operation mode is based on the MIHF (Media Independent Handover Function), which provides abstracted services to higher layers by means of a unified interface [14]. It exposes the service primitives that are independent of the Level 3 access technology, namely, the Service Access Points (MIH_SAP). For the media specific technology, each technology has its own link layer SAP, for better control over the handover performed.

The MIHF also provides three main services [2]:

- MIES (Media Independent Event Services), responsible for detecting events and delivering triggers from local and remote interfaces;
- MIIS (Media Independent Information Services), which provides the information model for query and response, making the handover decisions more effective;
- MICS (Media Independent Command Services), which provides a set of commands for the MIHF users to control handover relevant link states.

In the context of Figure 3.1, the Home/Visitor Core Network represents the service provider or enterprise. These providers offer access to their information server located in a MIH PoS node, in order for them to be able to obtain permanent information, like roaming lists, costs and provider identification information, although the MN can be pre-provisioned with these information.

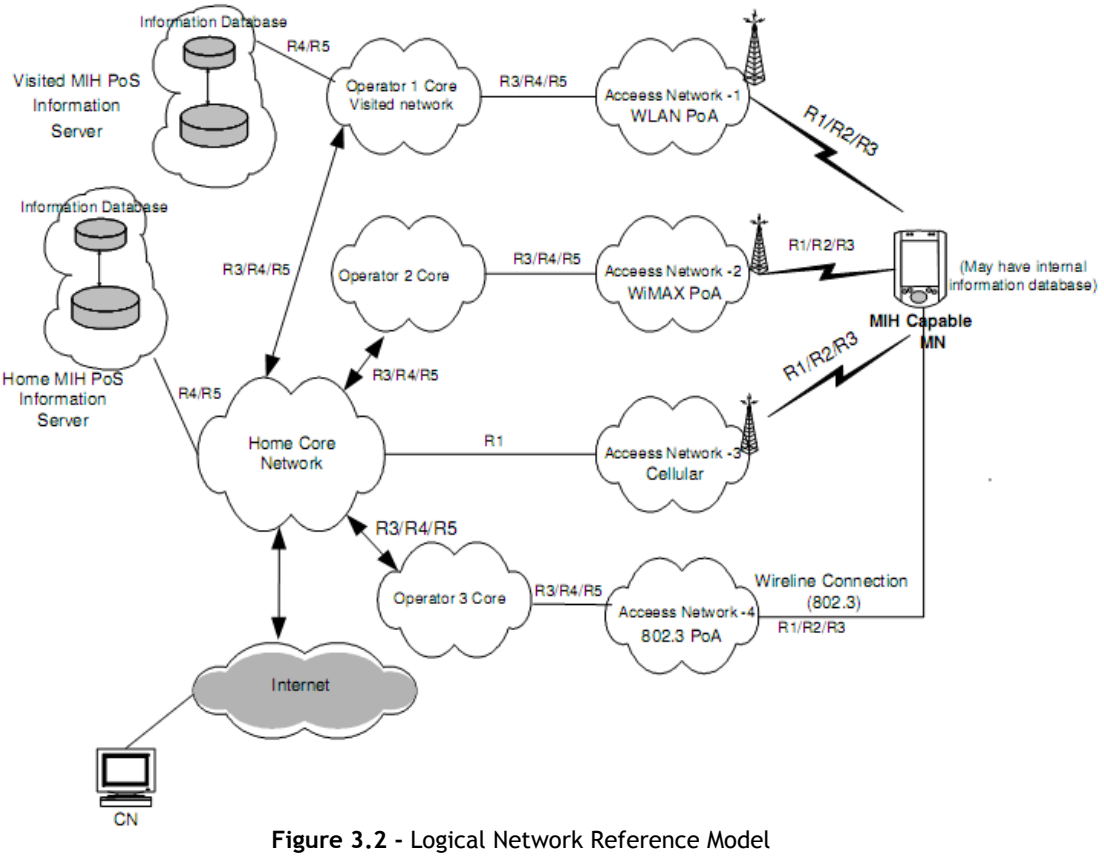

Figure 3.2 - Logical Network Reference Model

The Network provider offers MIH services in their access networks to facilitate handover. Each technology advertises its MIH capability or responds to MIH service discovery. Each service provider also provides access to one or more MIH Points of Service (PoS), which provide some or all the MIH services. The location of the PoS is not defined, it may be located next to the PoA, or deeper in the network.

The interaction between the visited and the home networks could be for control and management purposes, or for data transport purposes. It is also possible for the MN to connect to the Internet directly through the visited network.

3.1 Media Independent Event Service

Handovers may be initiated by the mobile node or by the network, due to the mobile node's mobility, state change of the environment, etc [2]. As these events occur, there are multiple higher layers that may be interested in the events. MIH can help distributing them. Events are treated as discrete, in some particular cases, the events have a state information associated, and as such, an *identifier* and other events may be associated with it.

The events are classified as either Link Events or MIH Events, depending on the destination and origin layers of the events, as can be seen in Figure 3.3. Events may also be generated locally or across the network. The Link Events are local in nature; however, the remote events are characterized by traveling though the network medium, from one MIHF to a peer MIHF.

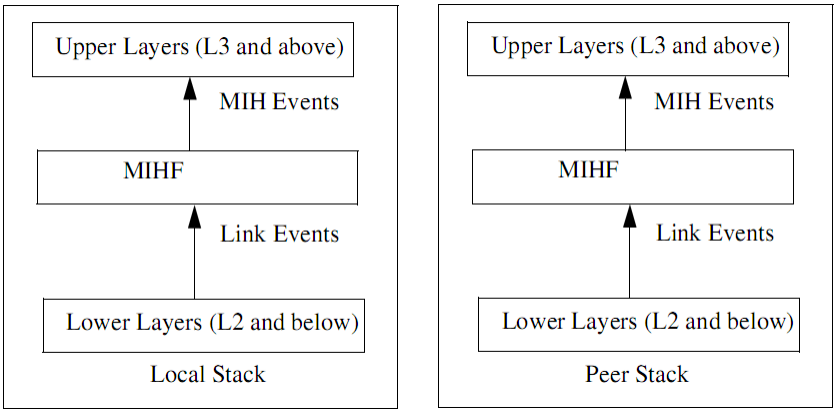

Figure 3.3 - Link and MIH Events

The Media Independent Event Service supports several types of events, as state change events, link parameter events, predictive events, etc. Independently of the type of events, there is a mechanism that permits upper layers to receive events selectively, provided by the event registration. Link Events registration is performed by the MIHF, but MIH events are registered by the upper layers with the MIHF, thus selecting the events to receive and possibly controlling the Event Service. With the information received by the events occurred, a MIH User may opt to use the Command Service, to control a handover. A Session ID is used

for the remote events, because it needs to be associated with the MIHF that keeps the subscription information.

3.2 Media Independent Information Service

As a mobile is about to move out of the current network, it needs to discover the available networks and communicate with the elements within these networks, to optimize the handover [14]. Considering the horizontal handovers, information provided by the lower link layers may be sufficient [2], in with cases information like the intra-technology neighbor reports is available from the access network. However, vertical handovers require a selection of the appropriate PoA in the network, base link connectivity and higher layer services, as well as session continuity for active user applications.

The Media Independent Information Service provides the capability for obtaining the necessary information for handovers, such as neighbor maps, link layer parameters, and higher layer services such as internet connectivity. It provides a schema, which helps to discover the capabilities of the MIIS, the different access networks and Information Elements (IE) supported by a specific implementation. The schema representation also allows the mobile node to query the information in a more effective manner, and it is defined by a language, which may be a Resource Description Framework (RDF) based on XML, Variants or a TLV representation. The MIIS schema may be classified in two categories, the basic schema that is essential for every MIH to support and an optional extended schema. The basic schema is not supposed to be updated, in opposition with the extended schema, which is intended to provide additional information, such as data structure and relationship of media-specific or higher-layer information.

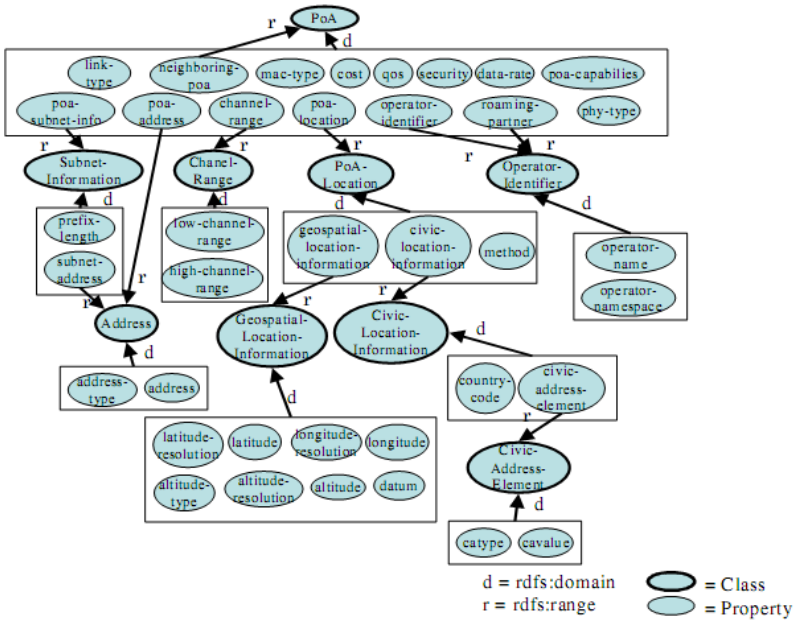

Figure 3.4 - A Representation of a Basic Schema

Information is provided by the MIIS about different access networks, which may be accessed from any single network. For instance, using an 802.11 access network, it is possible to access information about other 802.11 networks in the region and also other networks, like 3gpp, 3gpp2 and 802.16. The Information Service Elements [2] which provide this information are divided in three groups. The General Access Network Information provides a general overview of the different networks providing coverage within an area, which include a list of available networks and associated operators. The Information about Points of Attachment includes attributes of the PoAs in each of the available networks, such as PoA location and data rate supported. Other information is specific to a network.

Before a mobile node is authenticated with the new PoA, it should be able to obtain all the information elements available, which may be used to determine the appropriate PoA to connect. After the authentication and attachment to a PoA, the MIHF should have the knowledge that the network supports the 802.21 standard.

The information service provides access to both static information as well as dynamic information, present in some information server, or locally at the MN. Examples of static information [2] may include the names, providers and channel information of the mobile terminal's neighboring networks. Dynamic information may include parameters such as channel information, security information, and other information about higher layer services that will help make effective handover decisions. This information can be made available via both lower and upper layers. In some cases certain layer 2 information may not be available or may not be sufficient to make intelligent handover decisions. In such cases, higher-layer services may be consulted to provide additional information to assist in the mobility decision making process.

3.3 Media Independent Command Service

The Media Independent Command Service (MICS) [14] [15] uses the MIHF primitives to send commands from higher layers to lower layers. The MICS commands are utilized to determine the status of the connected links and also to execute mobility and connectivity decisions, and can be both local and remote. These include commands from the upper layers to the MIH and from the MIH to the lower layers.

The link status varies with time and node mobility [2]. As such, the information provided by the MICS is dynamic and comprises link parameters, while the MIIS is less dynamic or even static and refers network operators, between others. A combination between the information provided by them may be used in combination in order to facilitate the handover. In The MICS also provides two types of commands, as can be seen in Figure 3.5. These are called the MIH Commands and the Link Commands. As the MIES events, the MICS commands may also be local or remote.

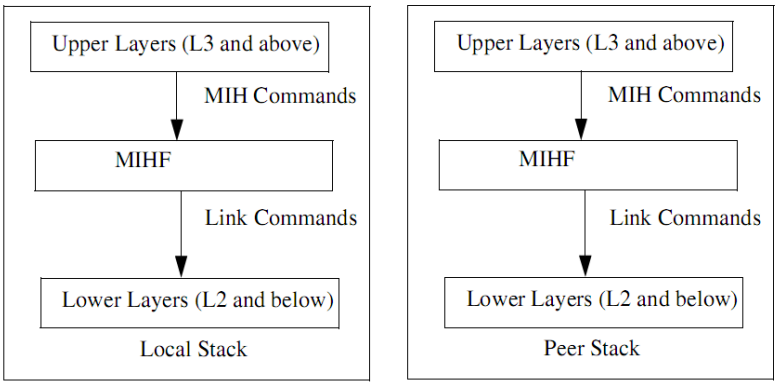

Figure 3.5 - MIH and Link Commands

3.4 MIH Access

There are at least three kinds of SAPs (Service Access Points), which provide synchronous and asynchronous services [1]. The MIH_SAP allows access from upper layers to the MIH, such as the MIH Link Up primitive that provides information on what state a L2 link is in, or the MIH Scan primitive which scans the network. The MIH_LINK_SAP provides an interface between the MIH and the network interfaces, like the Initialize primitive that initializes the MIHF or the Install Link primitive who informs the MIHF that a new link as been added to the mobile node or the network. The MIH_NMS_SAP allows management like the Link Up primitive that informs that the L2 connectivity is established or the Link Detected primitive that informs that a new link is detected.

Despite the fact that the SAPs referred are common for all interfaces, the MIH_LINK_SAP will only be possible if the access network technology allows MIH. Analyzing the access network, however, brings some conclusions [2]:

- 802.3 supports the MIIS, the MICS and the MIES, and uses the LSAP as an interface between the MIHF and the LLC (Logical Link Control).
- In 802.11, MIH is possible and it shall use some primitives like system configuration or link state change triggers. With this access technology, the LSAP is used when the client is associated with an AP, and the MLME before the station is associated.
- In 802.16, MIH is also possible and it shall use some primitives, like handovers, session management, radio resource management, etc. It also uses the M_SAP and the C_SAP, which are common between the MIHF and the NCMS (Network Control Management System).
- No new primitives are necessary to connect the 3GGP or the 3GGP2. The MIH can be mapped to existing 3gpp primitives.

3.4.1 802.11 MAC layer

The reference model in the 802.11 can be defined as can be seen in Figure 3.7, where the architecture of the 802.11 can be seen. However, for the implementation of the 802.21, there will be a need to introduce a SAP, the MLME_SAP, as can be seen in Figure 3.6.

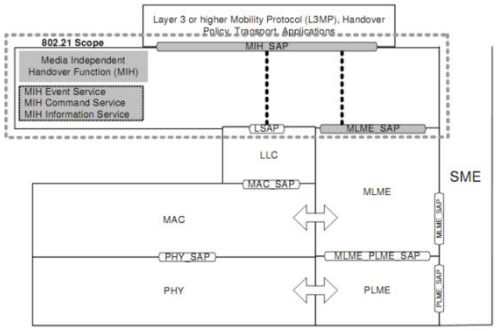

Figure 3.7 - MIH Reference Model in 802.21, for 802.11

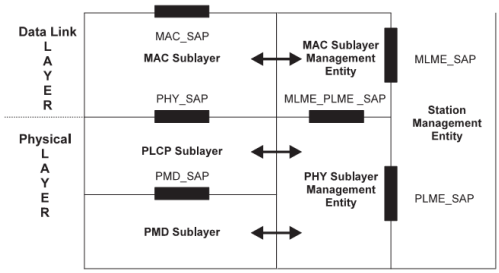

Figure 3.6 - Layers and Sublayers defined in the 802.11 basic reference model

3.4.2 802.16 MAC Layer

The MAC in the 802.16 includes three sublayers. The Service-Specific Convergence Sublayer, or CS provides the transformation or mapping of external network data received though the CS Service Access Point (SAP). The MAC Common Part Sublayer, or MAC CPS is the heart of the 802.16 MAC, and provides functionalities such as system access and bandwidth

allocation. The Security Sublayer provides functionalities related with authentication, secure key exchange and encryption.

The 802.16 MAC layer will need changes in order to support the 802.21. The changes consist only in the creation of the C_SAP and the M_SAP, which will provide an interface for the MIHF with the Network Management Entity.

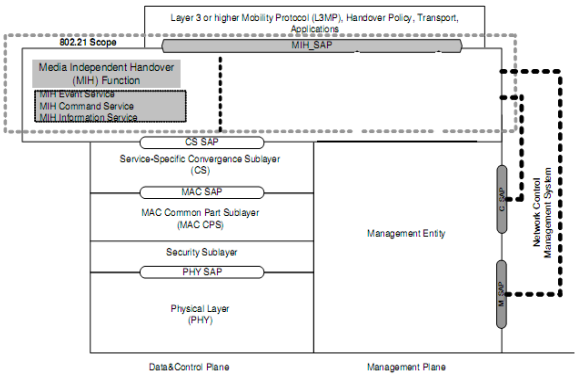

Figure 3.9 - 802.16 MAC layer

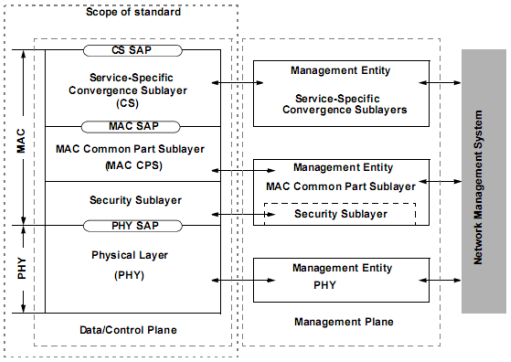

Figure 3.8 - Reference model in 802.21 for 802.16 MAC layer

3.4.3 3GPP Mac Layer

The 3GPP reference is used in order to implement the UMTS for the 802.21 structure. The 3GPP is an initiative from telecommunications standardization organizations to produce global specifications for the 3G networks, which include the Global System for Mobile Communications (GSM). No changes or new protocols/primitives are predicted to the 3GPP standard in order to implement the 802.21, at the MAC layer.

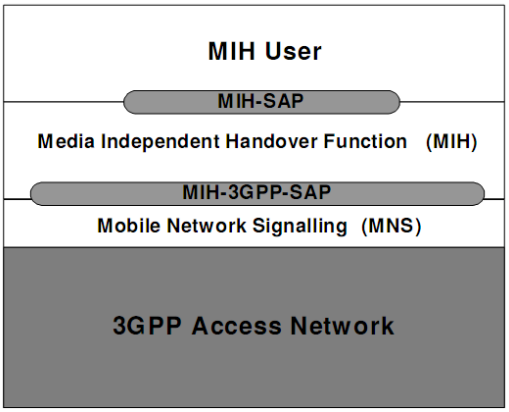

Figure 3.10 - 802.21 reference model for 3GPP

3.5 MIH Protocol

The MIHF sends and receives MIHF packets. These packets include information such as the Operation Code, Action Identifier, Service Type and Type-Length-Value containers. The Operation Code identifies the packet as a Request, Response or Identification; whereas the Service Type identifies the service the packet is sent for. The Action Identifier determines the type of MIHF packet, and also determines the quantity of TLV containers in the MIHF packet. The TLV containers are used in order to send data, such as a simple Boolean value, or a SPARQL query to retrieve information.

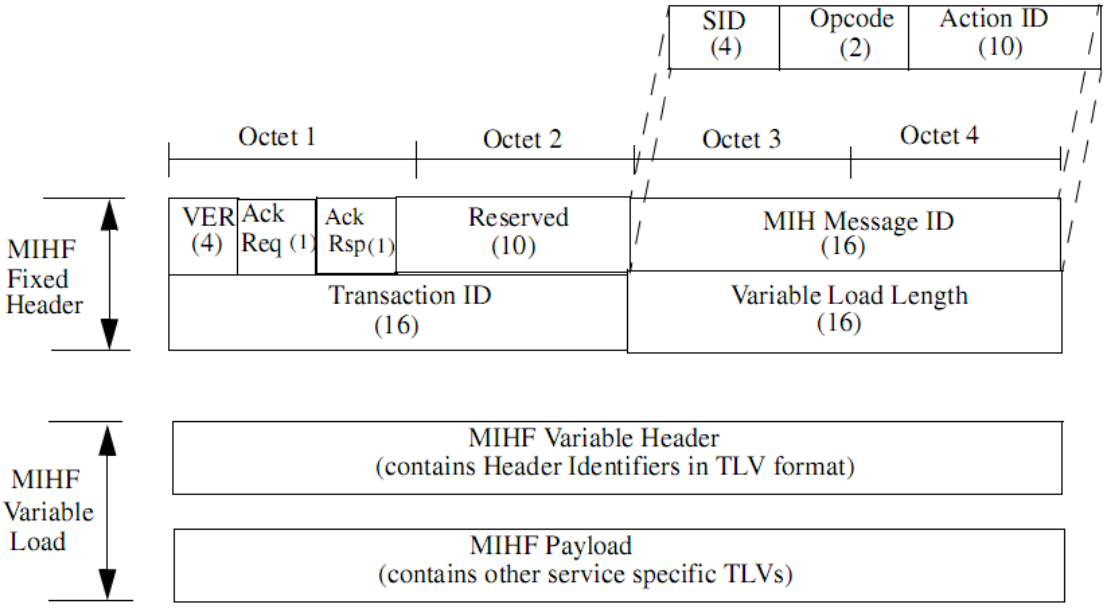

Figure 3.11 - MIHF Packet format [2]

Chapter 4

Implementation of a 802.21 Simulator Model for NS3

One of the main objectives in this project is to implement IEEE 802.21 in the Network Simulator 3 (NS3). It is an open source discrete-event network simulator, which is still in development. Each month, a new version of this software is released, which sometimes implies adaptation of the work developed to a new version. One of the main characteristics of the NS3 is the lack of a graphical interface, meaning that the work and implementation of codes and programs are made via C++. Relatively to the environment used, a NS3 programmer normally opts to work in a Linux or Linux-like environment, although there are programs to emulate a Linux shell in Windows, like Cygwin or MinGW, but need more testing.

The NS3 provides a few basic concepts in order to understand its processing. The following concepts are important not only in the NS3 terminology, but also in later chapters of this project [16]:

- Node. A basic computing device like a mobile terminal, is referred as a node, and is implemented in the C++ terminology by the class Node. In this sense, there is also a specialization of the class referred which is the InternetNode, and automatically provides a core IPv4 stack.
- Application. In NS3, there is no concrete concept of an operating system or system calls. But there is the concept of an application, which is implemented by a class with the name Application.
- Channel. A channel is defined as the media which connects a computer to a network. In NS3, it is possible to connect a Node to an object that represents the communication channel. This object is represented by the class *Channel*.
- Net Device. The net device terminology in NS3 covers both the drivers and the simulated hardware. It is possible for a node to be connected to more than one Channel via different Net Devices. The class NetDevice implements the net devices discussed in the simulator, providing methods for managing connections.

4.1 Visualization Module

The Visualization Module in NS3 has been developed using goocanvas, a library which uses a number of canvas items, required for the graphic visualization. The predefined graphical interface included the observation of the node mobility in the simulation scenario. Alterations were made in order to be able to see the mobile node's mobility though an area without Wifi access, to an area with Wifi Access. To accomplish this, the visualization module was changed in order to define a stationary node as a PoA, creating a new structure similar to the one presented for node mobility, and changing its parameters to show a different color and a different range. In the actualization process of the all the node's mobilities, the PoA also had to be distinguished, since it does not move.

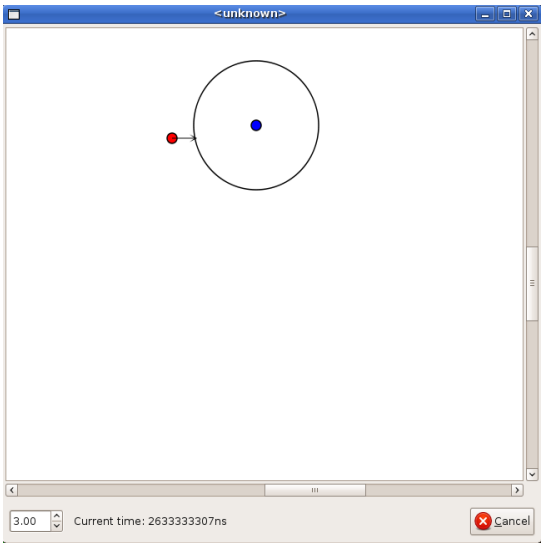

Figure 4.1 - Altered Visualization Module

4.2 Semantic Web

Using the conjunction of rules in the RDF Scheme, defined for the Media Independent Information Service, a set of subject – predicate – object parameters was defined in RDF. However, most of the attributes defined in the RDF Scheme are not necessary for this simulation parameter. A Simplification is shown in Figure 4.2, whereas information such as quality of service or security is not used and does not appear.

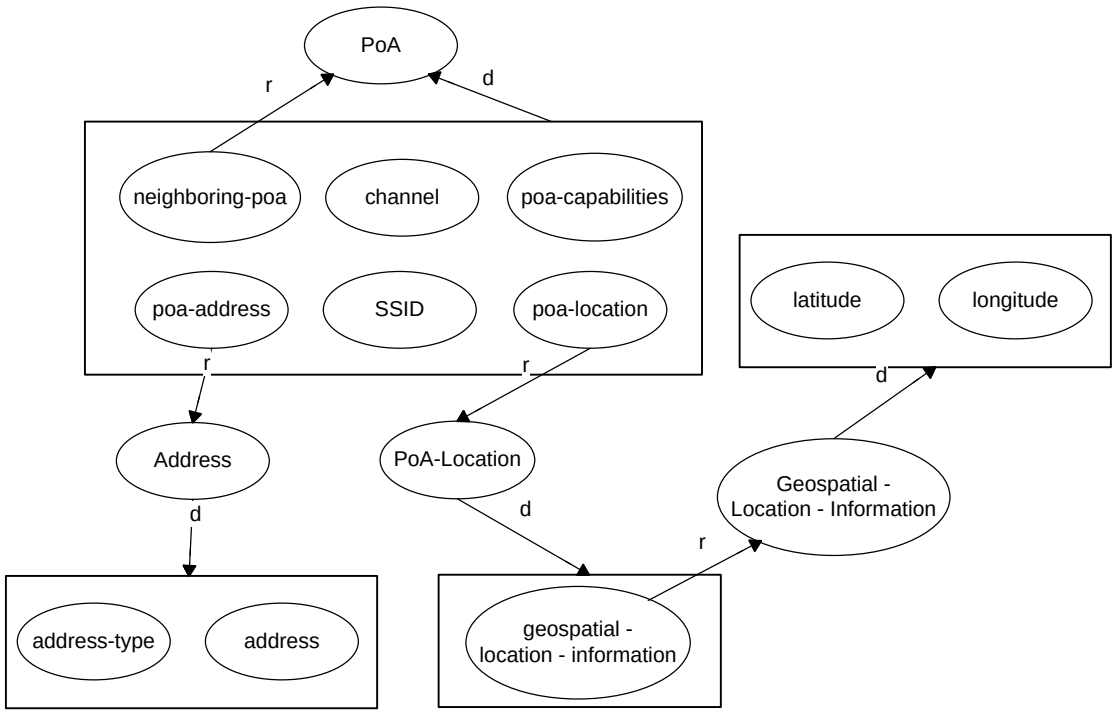

Figure 4.2 - Simplified RDF Model

As for the information defined in the RDF file, it was made using information based on a provisional scenario simulation. This information representation is only related to the Access Points. The simulation of the UMTS link by a Point to Point link, as will be possible to observe in later scope, defined that the UMTS PoA does not own a channel or a SSID.

```
<mihbasic:PoA rdf:ID="Node2">
  <mihbasic:neighboring-poa rdf:resource="&mihbasic;#Node0" />
  <mihbasic:mac-type>UMTS</mihbasic:mac-type>
  <mihbasic:poa-capabilities>1</mihbasic:poa-capabilities>
  <mihbasic:poa-location rdf:resource="&mihbasic;#Location2"/>
  <mihbasic:poa-address rdf:resource="&mihbasic;#Address12"/>
 </mihbasic:PoA>
```

Excerpt 4.1 - Part of a RDF File, defining the UMTS PoA

In order to use the RDF information in the NS3, an inclusion of a new library was necessary. The Redland RDF Library[1] was chosen to use this RDF information. The use of this library, however, also implies the use of a SPARQL query, for the retrieval of results. The implementation in the NS3 also included the creation of a new test program, in order to check the values retrieved from the RDF file. The Excerpt 4.2 shows an example of the retrieval of the UMTS PoA's MAC Address, from another MAC address of an Access Point in the vicinity of the UMTS PoA.

```
   std::string          teste          =          "PREFIX          mihf:
<http://www.pong.inescporto.pt/apinho/MIIS/RDF-Schema/>   PREFIX   xsd:
<http://www.w3.org/2001/XMLSchema#>      SELECT   ?mac   WHERE   {   ?x1
mihf:address "00:00:00:00:00:05" .            ?x2 mihf:poa-address ?x1
.                                        ?x2 mihf:neighboring-poa ?x3 .
?x3 mihf:poa-address ?x4 .             ?x4 mihf:address ?mac . } ";
```

Excerpt 4.2 - Example of an SPARQL query, for the retrieval of an MAC Address

The extracted results may be shown as the Excerpt 4.3 shows. In this example, a simple SPARQL query was made to retrieve only the MAC Address of the UMTS PoA, however, the structure of the results may be observed. The SPARQL query and the results will travel in a TLV packet, by request from the MIIS to the MIHF to query for results, or by the request from the MIIS to the MIHF to respond with certain results.

```
result: [mac=00:00:00:00:00:00]
```

Excerpt 4.3 - UMTS PoA's MAC Address retrieved from the SPARQL query

1 Site: http://librdf.org/

4.3 DHCP

In the simulation, a first approach to the problem represented by IP connectivity in handover was presented and solved by the use of a simple MIP configuration. But its solution is limited, due to the static IP configuration required for a communication to exist between a mobile Node and a Point of Access. A better and improved solution is the creation and use of a simplified DHCP. In this version, the client uses a DHCP Discover request, sent specifically to the MAC address of the PoA. It is acknowledged and responded, by the emission of information such as the new IP Address of the client, the network address and network mask, the clients default gateway, i.e., the Point of Access. As will be possible to observe, the MAC Address required in this implementation is available within the RDF file available to the mobile node.

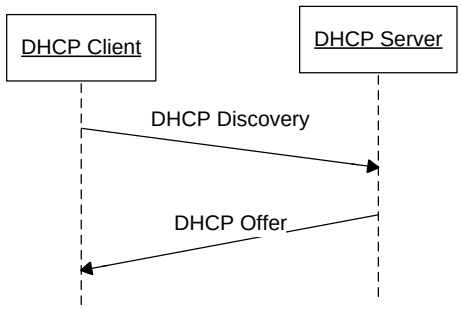

Figure 4.3 - Simplified DHCP Message Exchange

The structure of the UDP-Echo Application was used as a basis to implement the DHCP. As such, the DHCP application uses the NS3 socket class to send and receive values. For the definition of the destination parameters, such as the MAC Address of the DHCP Server, the NS3 PacketSocketAddress was used. Finally, the DHCP Server provides the parameters to the DHCP Client based on the default parameters provided, by a DHCP header frame, which uses the NS3 Header class. This DHCP frame has also been simplified, and only provides the IP Address of the DHCP Client, the network address and mask and its own MAC Address.

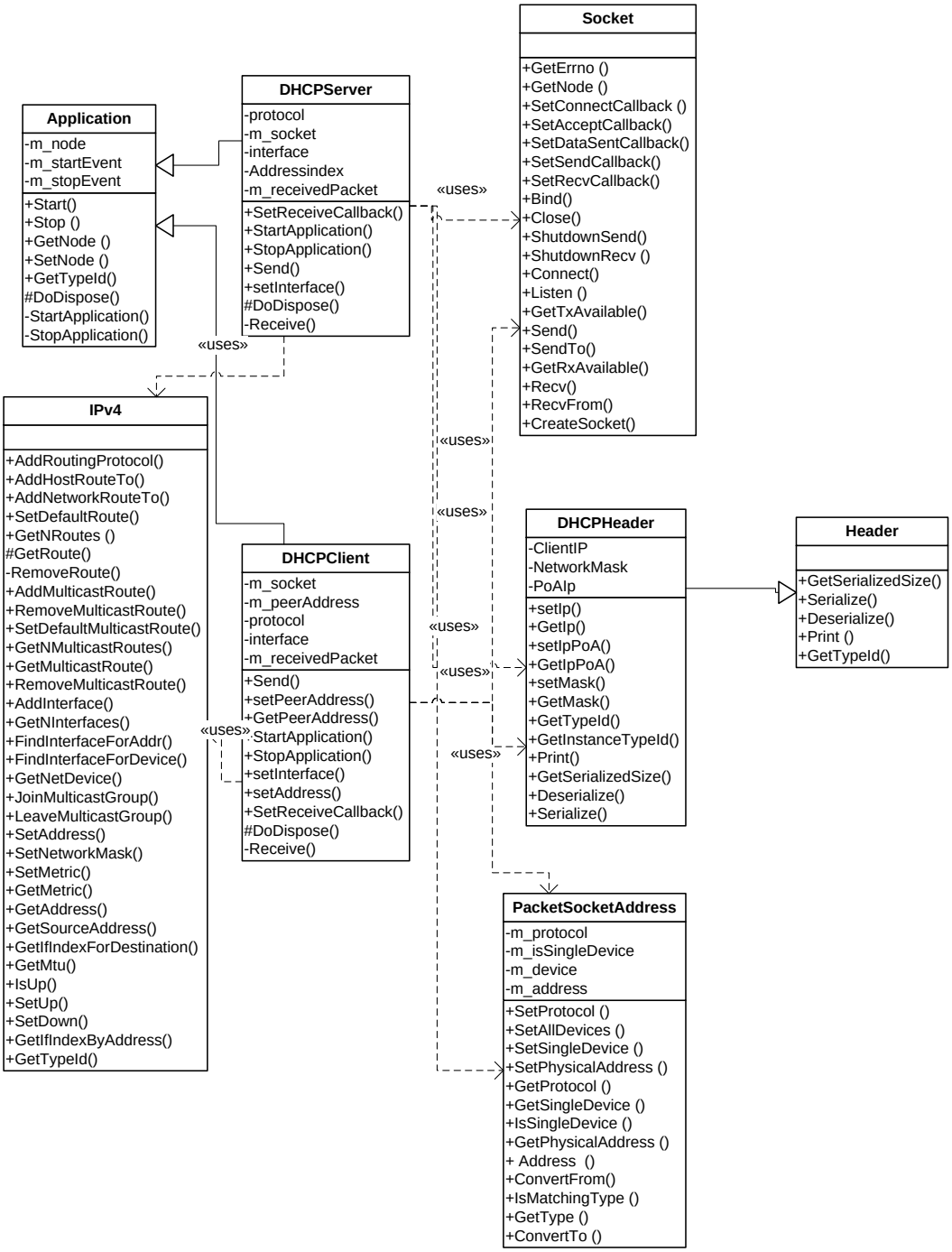

Figure 4.4 - DHCP Classes Diagram

4.4 MIHF

Meant to be without any “intelligence”, the MIHF module is aware of the existence of a defined Wifi interface, which is defined in the creation of the application in the Mobile Node. The PoAs and the Server do not need to specify this interface, since it may not even exist. From this Wifi interface defined, the MIHF listens to events from the Wifi Net Device, transmitted by NS3 callbacks. Two default callbacks are used by the MIHF to active awareness of the Mobile Node’s Wifi link state: the Wifi Link Up callback, and the Wifi Link Down callback. Upon these two callbacks, the MIHF chooses to transmit the warning to an upper layer, by the same callback system. However, if the Wifi Link Up callback occurs, the MIHF also transmits a MIHF packet informing the network that a Wifi link as been detected.

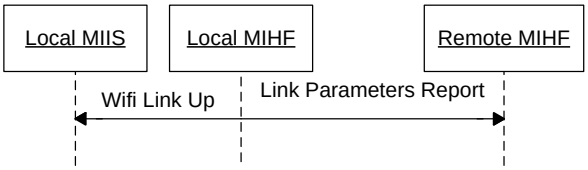

Figure 4.5 - Wifi Link Up Notifications

Further callbacks are used to detect the transmission and receive status of the Wifi Link. These callbacks are useful for determining another even that should occur, the Wifi Link Going Down callback, which is not implemented in the Wifi callback. However, the Wifi link is not prepared to detect frames that were lost due to transmission errors, before the Mobile Node exits the PoA range. Due to this fact, a handover scenario which includes the Wifi link as a starting link interface is discarded, since no frames can be transmitted to the PoA before the Wifi link is disconnected.

The registration for remote link events has not been implemented. It is not an objective, since the only event of relevance to the framework implemented and to demonstrate the importance of the 802.21, is the Wifi Link Up Event. This event is always registered in the Mobile Node, for the connected PoA. The Wifi Link Going Down event is also prepared however, it could not be tested properly and is not registered with the remote MIHF.

In order to implement the Wifi Link Going Down Event, and the Wifi Link Rollback Event, a set of variables where defined to determine the current status of the link. These variables can be characterized by counting the received packets, the received packets with errors and the received packets successfully.

(4.3) $$currentStatus = \frac{rx\_ok}{rx\_ok + rx\_error} * 100$$

If the current status variable was superior than 60%, and becomes less than 60%, a Wifi Link Going Down is generated by the MIHF. However, if the opposite occurs, and a Wifi Link Going Down was generated by the MIHF, a Wifi Link Rollback takes place.

The variables used tend to increase each time a packet is received. A error could occur if a Mobile Node is stationary for a long time in the range of the Wifi PoA, and then leave its range. In this example, the MIHF would have a great number of successfully received packets, and low packet error. The MIHF's Mobile Node could not detect correctly the Wifi Link Going Down under these circumstances. To correct this possibility, a function is scheduled to occur within the NS3 Simulator with a pre-defined interval, for the re-definition of these variables with its default parameters.

The MIHF controls in the NS3 enterprise commands such as the MIHF Switch, which treats the connection of the new link and the disconnection of the old link, valuable to the handover process. The handover process is not made by the MIHF, but commands such as the MIHF Switch provide some control over it. As a control frame, one may also consider the transmission of MIHF packets, which may be requested by upper layers. These MIHF packets are sent to the destination defined, which may be defined on the start of the application, or by another command.

As a special note to the diagram in Figure 4.6, one may refer that the TLV container is implemented by the TLVPacket class. Also visible in this diagram, is the amount of primitives made for the MIHF communication, such as the CapabilityDiscoveryRequest. This primitives use their parameters to configure and send a MIHF Packet to a pre-determined destination. Another two classes used by the MIHF are the IPv4Address and the Mac48Address. However, these were not referred for the simplification of the diagram. The NS3 Packet class is also not referred, since it is implicitly defined whenever the socket class is used.

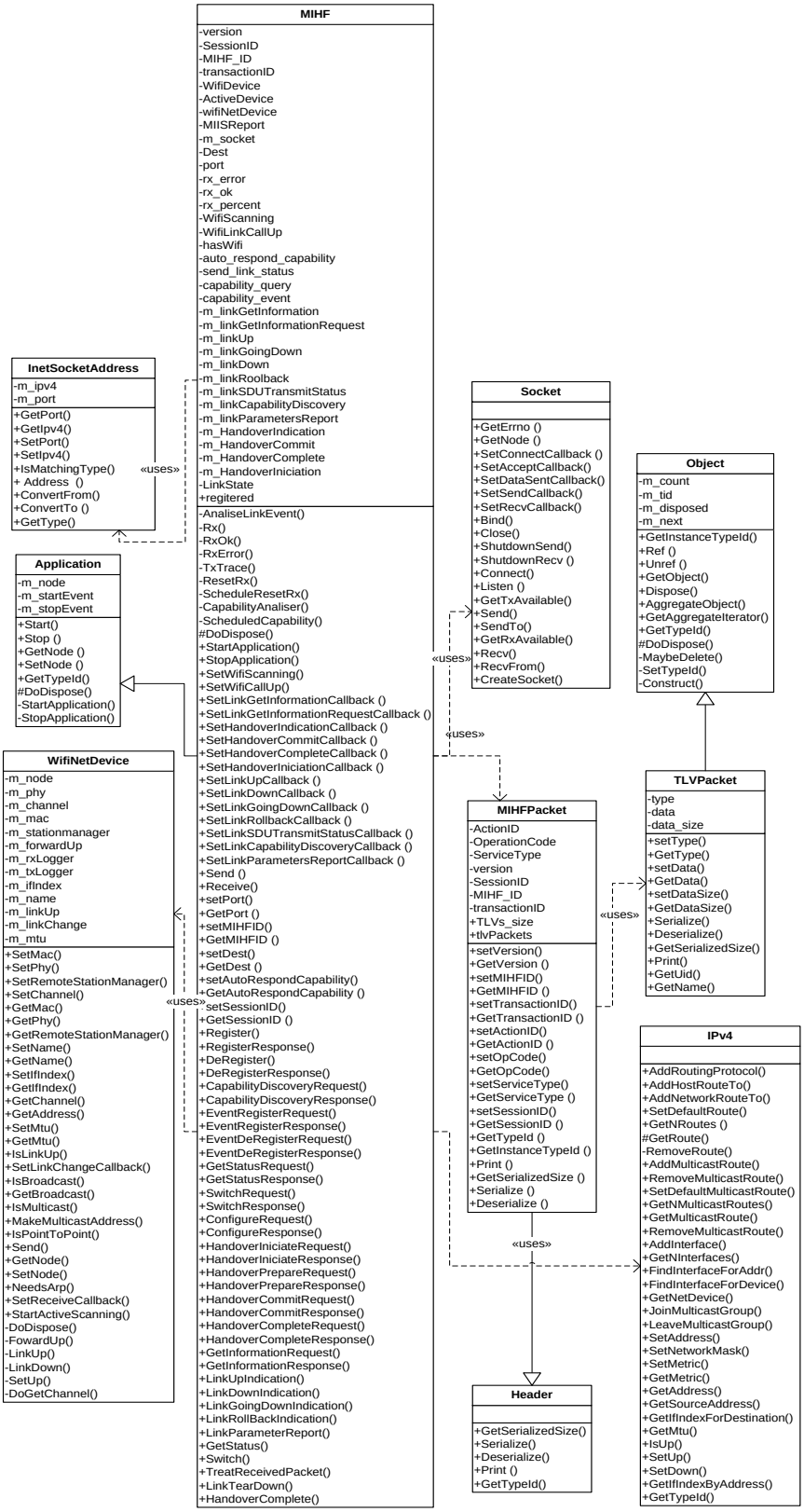

Figure 4.6 – MIHF, MIHFPacket, TLVPacket Class Diagram

4.5 MIIS

The MIIS module is separated from the main MIHF. This happens because the MIIS is meant to be a MIHF User, using the MIHF for retrieving information and analyzing it. The information retrieval from a RDF file is also made by MIIS, in this case, the MIIS Server. This server comprises the minimal MIHF, needed only to acknowledge or deny MIHF Capability Discovery requests, or to respond to the SPARQL queries received.

In Figure 4.7, one may observe not only the use of the MIHF by the MIISServer application, but also the RDF parameters needed for the use of the SPARQL query. Also, for simplification of the diagram, the operations and attributes of the already referred MIHF class are resumed.

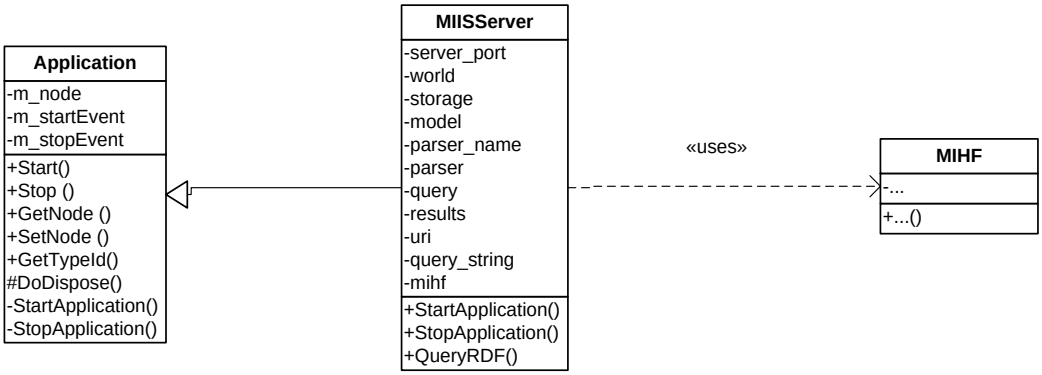

Figure 4.7 – MIISServer Class Diagram

The information necessary for the handover process is retrieved via a SPARQL query, enclosed in a TLV container, and sent to the MIIS Server. The Server uses the query and retrieves results from the RDF file, returning them to the MIIS PoA, which caches the results for analyses and to send them to the stations that request information. The request for information by the MIIS PoA is made in the beginning of the simulation.

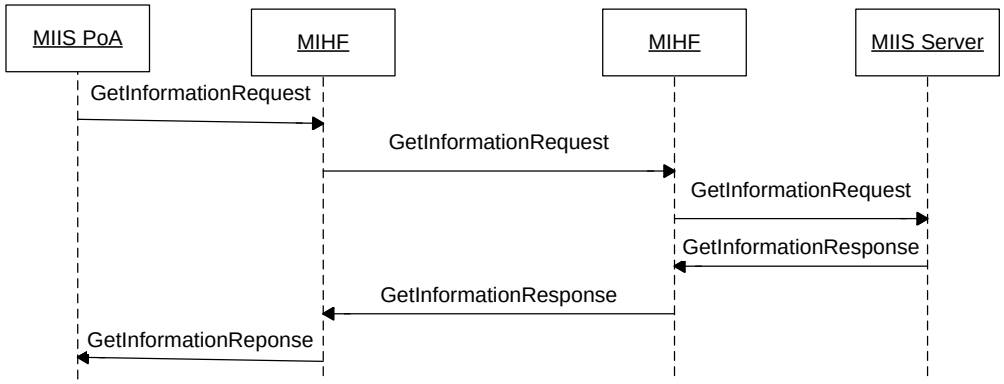

Figure 4.8 - MIIS PoA Get Information Scheme

The query for information may depart from both the PoA and the Mobile Node. It is assumed that the Mobile Node always requests information about the neighboring PoAs, and queries the PoA it is connected to. In result, although the Mobile Node is making a query, the PoA always responds with the information relevant with the PoAs in the neighborhood. If the MIIS PoA does not have the results available, it will query the MIIS Server for an information report. The information reports and queries are made in the beginning of the simulation by the Mobile Node, or after a handover has been performed. In this scenario, a MIIS Client, or the application in the Mobile Node, is designated as an MIIS Station.

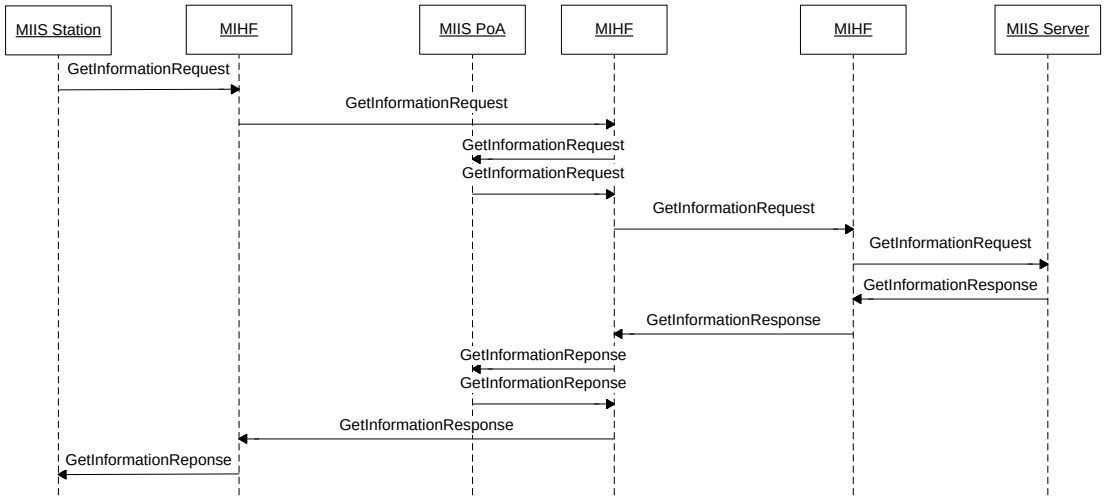

Figure 4.9 - MIIS Query and Response with no cache in the MIIS PoA

In the implementation made, the MIIS module also works as a mobility agent, using the DHCP to perform the IP configuration after the handover is made. This is used in the MIIS PoA and in the MIIS Station, in the handover process. Also in this process, the PoA determines which neighboring PoA is in the range of the Mobile Node, based on the information obtained from the MIIS Server in the beginning of the simulation.

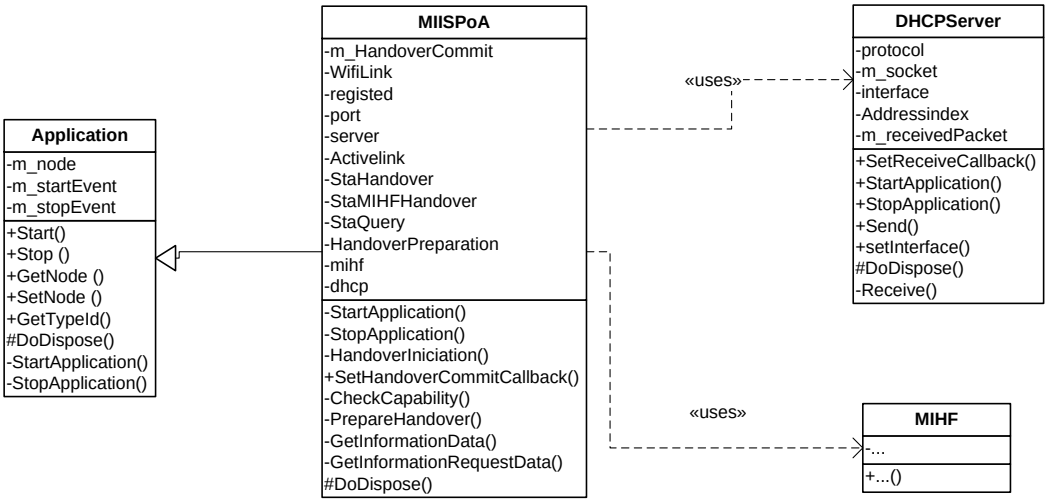

Figure 4.10 – MIISPoA Class Diagram

In another analysis, the MIISSta class, which implements the MIIS Station, is prepared to perform and control the handover. It also launches the DHCP configuration process, when the Mobile Node switches interfaces, working a mobility agent. If there is a handover to a Wifi link and there is no information available of it, the MIIS Station is also prepared to perform a scanning on all Wifi channels available.

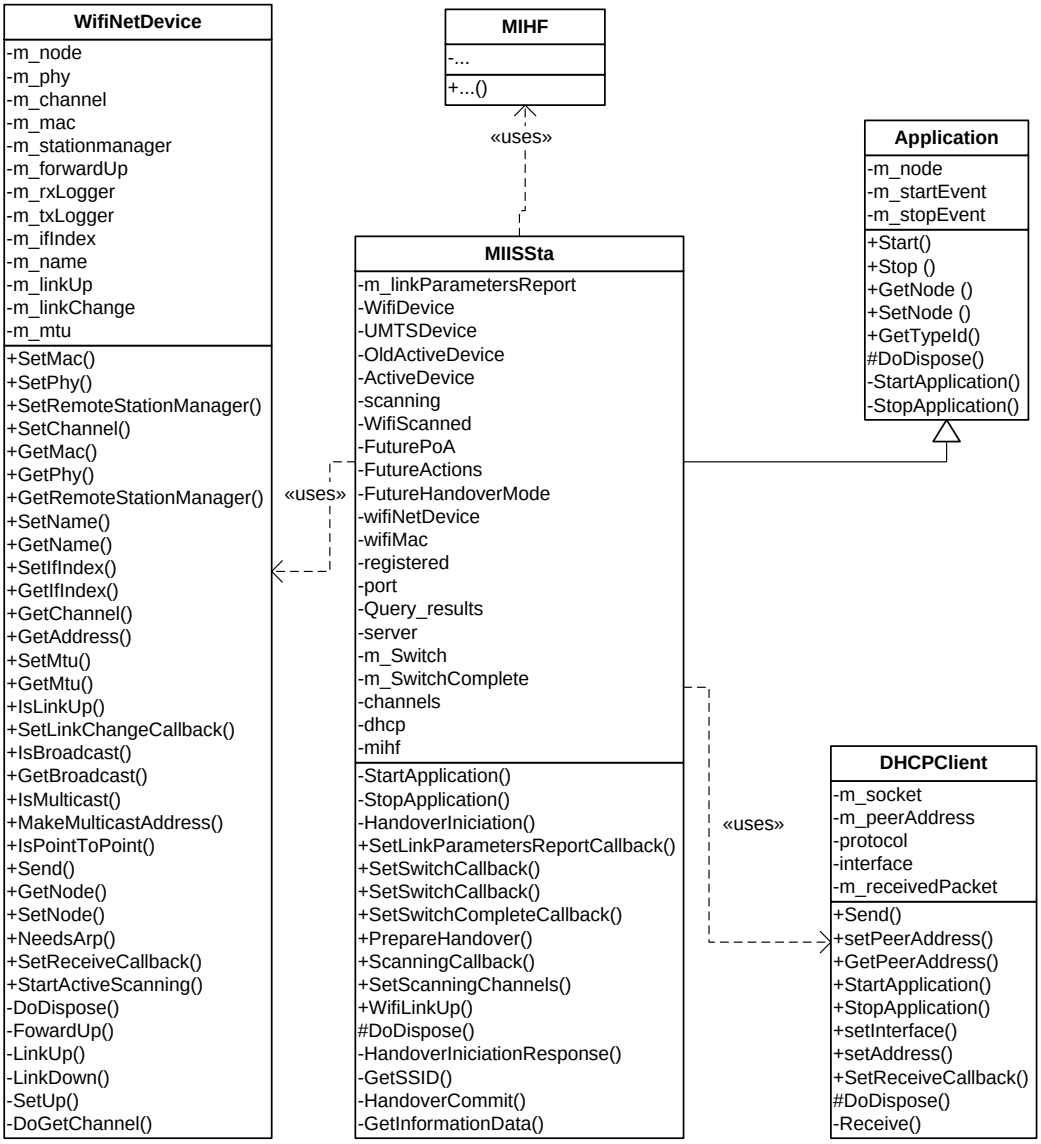

Figure 4.11 – MIISSta Class Diagram

The MIIS has been made to complement and improve the MIHF, not only though the information available, but also by providing handover control. This is made by retrieving information such as a Wifi Link available and performing the necessary controls. In the work developed, the handover decision is made by the network when it verifies that there exists another link available. The controls executed to perform the handover with success also include the DHCP commands to obtain the Mobile Node's new IP address, and its report to the MIIS Station.

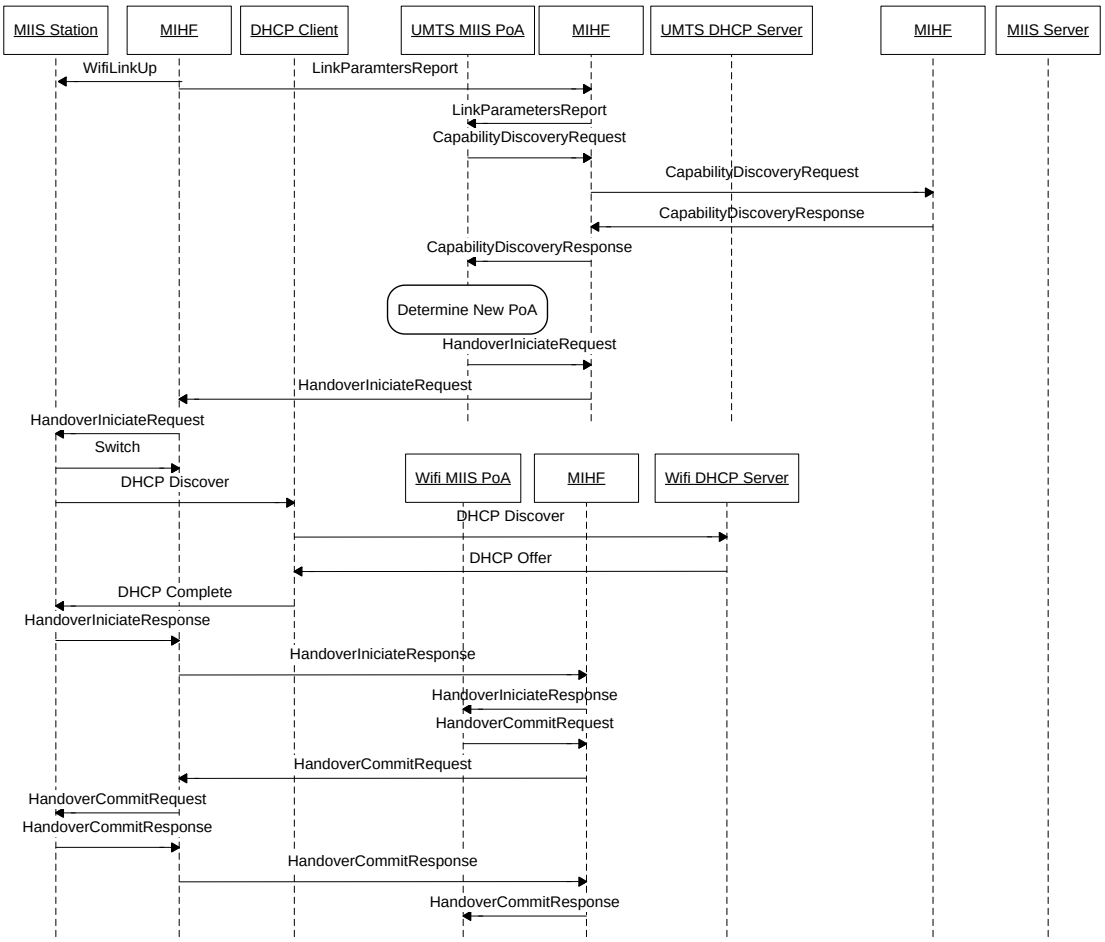

Figure 4.12 - Module Intercommunication in a UMTS - Wifi Handover

Using the example shown in Figure 4.12 for a handover between UMTS and Wifi, it is possible to describe the handover process. It begins with a detection of an available Wifi link, and its report to the network and to the Mobile Node's upper layers. Upon receiving the MIHF packet which informs the network of a new link, the UMTS PoA queries the MIIS network server of the availability of MIHF in the Mobile Node's network, through a MIHF Capability Discovery request. After receiving its response, the UMTS PoA determines the most suitable link available for the Mobile Node, and reports to it through a Handover Initiate Request. The Station changes interfaces, and requests the DHCP to configure the IP Address and connectivity through a DHCP Discovery command. When the DHCP acknowledges the new configurations, it informs the Mobile Node, which informs the Wifi PoA that the handover initiation has been completed. Finally, the Wifi PoA requests to commit the Handover, which is made by the Mobile Node.

Chapter 5

Simulation and Study of an 802.21 Based Handover Scenario

The main objective of the project is to implement the IEEE 802.21, in the Network Simulator 3, although the IEEE standard is still not finalized. This standard and its implementation has the objective to perform vertical handovers. This chapter describes simulation studies to evaluate the time taken to perform a handover successfully, in and between the network access technologies chosen.

The chosen scenario is the handover between the UMTS link and the Wifi link. Despite the consideration in the implementation of a handover from the Wifi link to the UMTS link, it was soon discarded, since the handover to the UMTS link cannot provide different results with or without the MIHF. In order to implement the scenario, the UMTS link has been simulated via a point to point link. Both the UMTS PoA and the Wifi PoA are connected to the MIIS Server, through a single CDMA interface. This interface will help determine the handover times from a packet flow created.

When the Mobile Node detects the Wifi link available, it will attempt a handover to it. This Wifi link has been configured so that the PoA broadcasts the Beacon Frame, and that the station does not perform an active probing until requested by a scanning procedure. The Wifi Station is also pre-configured with the channel and the SSID of the Wifi PoA, in order to perform a make-before-break handover. Further configurations in the Wifi link include power levels, fragmentation and rts/cts thresholds.

Table 5.1 - Wifi Parameters Used

Parameters	Values
Wifi PoA	
Beacon Generation	True
SSID	INESC
Mobile Node	
Active Probing	False
SSID	INESC
Wifi Remote Station Threshold	
Fragmentation Threshold	2200 bytes
RTS CTS Threshold	0 bytes
Wifi Phy	
Rx Gain	-10 db
Tx Gain	-10 db

The DHCP has been configured in the UMTS PoA and in the Wifi PoA. In the UMTS PoA, the network has been defined as a 10.20.0.0/28 network, while in the Wifi PoA, the DHCP has been defined to a 10.16.0.0/24 network. The DHCP Protocol parameter, needed by the class PacketSocketAddress of the Network Simulator 3, has been defined as 2. The DHCP Client has been initialized with its first link configuration, referred to the UMTS link, although this was not necessary, due to the alteration of this value by the MIIS, in the handover process.

Table 5.2 - DHCP configuration

Parameters	DHCP Client	DHCP Server
Protocol	2	2
Address	-	10.16.0.6 10.20.0.1
Interface	-	Interface Index

The MIIS general configuration consists in the definition of the MIHF Port for communication, port 10'000. The MIIS PoA also requires the IP Address of the MIIS Server and the Active link to control, besides the pointer to the DHCP Server created. As for the MIIS Station, installed in the Mobile Node, this NS3 application needs certain requirements: the MIHF Port, as Port 10'000, the pointer to the DHCP Client application, the IP Address of the PoA it is connected to, the Active Device which is connected to the PoA, the index values of the two configured devices, UMTS device and Wifi Device, the Pointers to the WifiMac class and to the WifiNetDevice class.

Table 5.3 - MIIS configuration

Parameters	MIIS Station	MIIS PoA	MIIS Server
Port	10'000	10'000	10'000
Server Address	10.20.0.2	10.1.0.1	-
Active Link	UMTS Device index	UMTS/Wifi Device index	-
DHCP	Client	Server	-
Wifi Device	Wifi Device index	-	-
UMTS Device	UMTS Device index	-	-
Wifi Net Device	Wifi Net Device used	-	-
Wifi Mac	Wifi Mac used	-	-

The mobility in this scenario consists is twofold. The MIIS Server and the UMTS PoA are stationary and located in a special location, so that they do not appear in the visualization window. The Wifi PoA is also stationary, and is located at (x,y) = (100, 20), appearing in the visualization window with its Wifi range. As for the Mobile Node, it uses a Waypoint Mobility Model, starting at (x,y) = (40,25), and ending at (x,y) = (200, 25). With these parameters, it will be possible to observe the Mobile Node entering the range of the Wifi PoA, being expected that it will perform a handover from the UMTS link to the Wifi Link.

Table 5.4 - Mobility Configuration Parameters

Parameters	Mobile Node	UMTS PoA	Wifi PoA	MIIS Server
Mobility Type	Waypoint	Static	Static	Static
Start Location	(40.0,25.0,0.0)	(-100'000,0.0,0.0)	(100,20.0,0.0)	(-100'000,0.0,0.0)
End Location	(200.0,25.0,0.0)	-	-	-
Speed	10.0	-	-	-

In order to be able to perform a scanning, the definition of twelve Wifi channels has been made. The Wifi PoA is configured to use one of these channels. The Mobile Node may use the information provided in the RDF query response to connect to a channel, or perform a Wifi scan on them to determine which one to connect.

To obtain results, the presence of the SSID in the RDF file determines if the Handover will be made using the MIHF, or without the MIHF. The simulation of the Wifi link will be done with a simulation of traffic inducing Wifi stations, of about 1 Mbit/s.

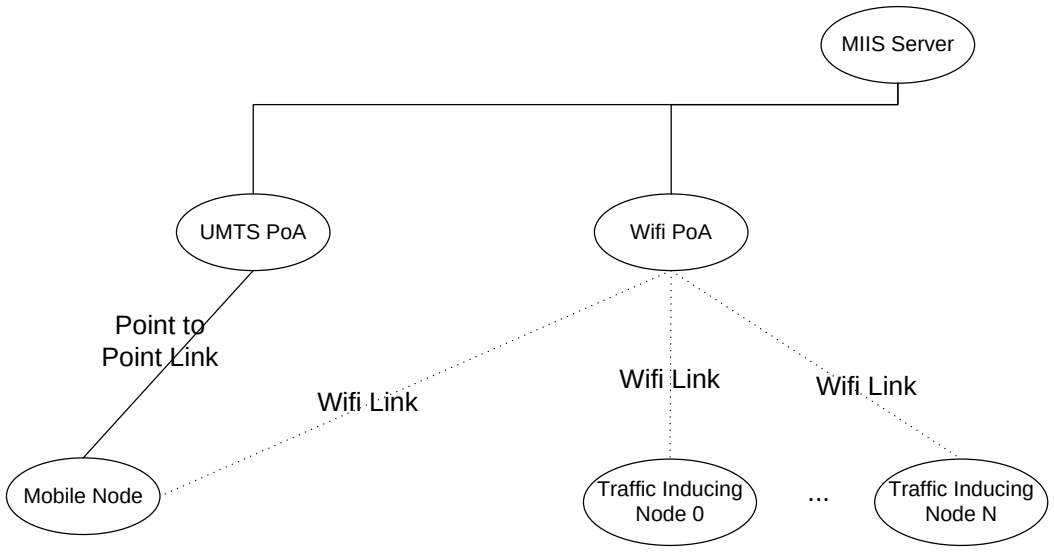

Figure 5.1 - Network Simulation Scheme

With this default configuration, and considering the make-before-break handover predicted, the handover time expected should be twice the Round Trip Time, the value expected for the DHCP frames to arrive from the Mobile Node to the PoA, and from the PoA to the Mobile Node. Considering an acceptable Round Trip Time of about 10 ms, a MIHF handover should take about 20 ms. As for the handover without MIHF, this should take a while longer, due to the scanning the Mobile Node, the authentication and association procedures needed before the DHCP frames are used.

5.1 Handover with MIHF

Using the connections and routing between all nodes in the network, an UDP packet flow was created from the Mobile Node to the MIIS Server. Each packet uses the port 200 and has the size of 10 bytes. The time between each packet transmitted is 10 ms. Using this parameters to calculate the handover time, it can be extracted by the visualization of the time taken to receive the packet flux from the UMTS IP Address, to the Wifi IP Address.

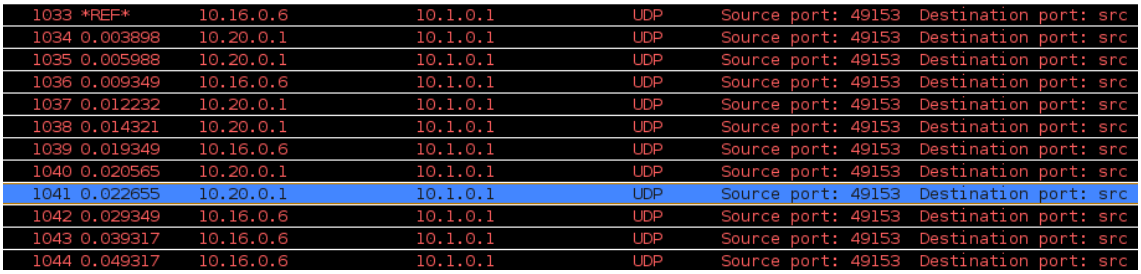

Figure 5.2 - MIHF Handover With no Traffic inducing Nodes

Table 5.5 - MIHF Handover times with Wifi Traffic inducing Nodes

Traffic inducing Nodes	Handover Times
0	0.009972
1	0.009972
2	0.009972
3	0.014490
4	0.014323

As can be seen, the handover with MIHF is seamless, i.e., the Mobile Node's User does not realize the handover is performed due to the small handover time. However, without MIHF, the Wifi channels must be scanned to acknowledge which is the channel the Mobile Node will

connect to. This handover time is larger, and takes about 0.59 seconds to be performed, when there are no Wifi stations inducing traffic.

The relevance of the RDF file is of great importance in the handover within MIHF. The presence of information which includes the location of the PoA and its SSID, for instance, not only helps but reduces the handover time, making the handover, a make – before – break handover type, establishing the L2 link configuration before the handover is made.

```
<mihbasic:PoA rdf:ID="Node0">
  <mihbasic:neighboring-poa rdf:resource="&mihbasic;#Node2" />
  <mihbasic:mac-type>Wifi</mihbasic:mac-type>
  <mihbasic:ssid>INESC</mihbasic:ssid>
  <mihbasic:channel>0</mihbasic:channel>
  <mihbasic:poa-location rdf:resource="&mihbasic;#Location0"/>
  <mihbasic:poa-address rdf:resource="&mihbasic;#Address10"/>
</mihbasic:PoA>
```

Excerpt 5.1 - Part of an RDF File, defining the Wifi PoA

The retrieval of information is made by a SPARQL query. In it, one may create the standard prefixes, and select the attributes wanted. The following parameters define the triples subject – predicate – object, which are necessary to specify the wanted results.

```
PREFIX mihf: <http://www.pong.inescporto.pt/apinho/MIIS/RDF-Schema/>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> SELECT ?ssid
?latitude ?mac ?longitude ?channel WHERE { ?x1 mihf:address
"00:00:00:00:00:00” . ?x2 mihf:poa-address ?x1 .
?x2 mihf:neighboring-poa ?x3 . ?x3
mihf:poa-address ?x4 . ?x3 mihf:poa-location ?x5 .
?x5 mihf:geospatial-location-information ?x6 .
?x6 mihf:longitude ?longitude . ?x6 mihf:latitude
?latitude . ?x4 mihf:address ?mac . OPTIONAL {
?x3 mihf:ssid ?ssid . ?x3 mihf:channel ?channel . } . }
```

Excerpt 5.2 - SPARQL query example, for the UMTS PoA

When the SPARQL results are sent, in this case, to the Mobile Node, one may observe the most important parameters in a PoA: location, Wifi channel, SSID and MAC address. For simplification, the UMTS PoA is assumed to be at location 0:0, and does not own a SSID or a Wifi channel.

```
 [ssid=NULL,     latitude=0,     mac=00:00:00:00:00:05,     longitude=0,
channel=NULL]
```

Excerpt 5.3 - SPARQL Query example, for the UMTS PoA

The RDF information available justifies the seamless handover, but does not justify the time spent to perform the handover. This may be justified by the round trip time taken for the DHCP frames to reach their respective destination. In such process, considering a round trip time of about 10 ms, it should take about 20 ms to perform the handover. However, another consideration must be made: while the Mobile Node is performing the handover, the UMTS PoA still has packets in its queue and is transmitting them to the MIIS Server's node. So, even if the considered and predicted handover should take about 20 ms to occur, it is not possible to verify this value.

Another parameter that may be observed is referred to the handover times with three or more nodes. This time is bigger than the ones that occurred with fewer nodes, probably due to a channel occupation when the Mobile Node tries to transmit the DHCP frames and the channel is already occupied. This characteristic also explains why the handover may fail when there are three or more traffic inducing nodes, by the attempt to transmit the DHCP frames and its failure after a certain timeout.

There are also three packets which are lost in the handover procedure. One of packets lost may be justified due to disconnection of the UMTS link when the packet is still being transmitted. The other two packets lost may be justified by the functionality of the Wifi Network Device's queue in the Network Simulator 3, which does not condone with the emission of multiple packets at the same time. In this scenario, the MIHF Handover Initiate Response suppresses both the packets from the flux. Although another consideration could be done, assuming that these packets lost where due to the disconnection and emission of packets from the Mobile Node, while this was disconnected, this assumption is incorrect, as will be possible to observe in the handover without MIHF.

5.2 Handover without MIHF

Considering a handover that does not use the MIHF, there is a need to perform a Wifi scanning before determining the channel to connect to. This scanning also determines the PoA SSID and MAC Address, needed for the DHCP to take place. Using the active scanning equation already seen, this handover time should take about 600 ms, due to the twelve channels needed to scan.

(0.4) $$ScanningTime = 50ms * 12 = 600ms$$

The results expected are of 600ms, due to the scanning phase only. The authentication and association procedures are not considered, in order to simplify the process, and since the most time expending procedure is the scanning method. The same may be referred to the DHCP frames needed for the configuration of the IP parameters of the Wifi device, after a handover.

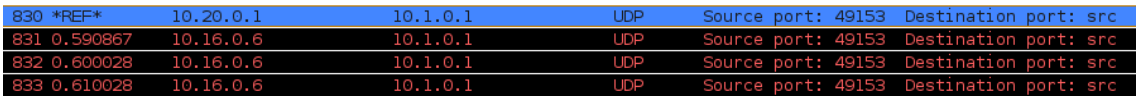

Figure 5.3 - Handover With no Traffic inducing Nodes and without MIHF

Table 5.6 - Handover times with Wifi Traffic inducing Nodes without MIHF

Traffic inducing Nodes	Handover Times
0	0.590867
1	0.640946
2	0.590946
3	0.590918
4	0.59085

The scanning procedure in this handover type indeed determines the outcome of the handover time. In the results, one may observe results of about 0.59 seconds. This is the contribution of both the scanning, and the packet transmission delay, i.e., when the Mobile Node starts the handover, the UMTS PoA still has packets in its queue. Another reference may be made to the handover time of 0.64 seconds. This result occurred due to an frame transmission failure, in which the Mobile Node tried to connect to the PoA, and it failed. This transmission failure may be from the association method, from the authentication method, or even from the DHCP method.

Referring to the packet loss in this handover type, it may be observed that not one packet was lost in this handover, not even the ones lost previously in the MIHF handover; in the process of disconnecting the UMTS interface. This may happen because the packets were transmitted successfully before the UMTS interface was disconnected. However, since no further packets are sent by the MIHF, no packets are lost due to the warning and configuration methods required in the MIHF.

When there are three or more nodes inducing traffic in the Wifi link, the handover time may not be obtained, since this is not performed. Under these circumstances, the traffic in the Wifi link may be great enough for the loss of one of the DHCP frames needed. Simulation of more than 4 nodes has been discarded, because the objective of this simulation is to test the performance of an handover with a high traffic network, with low frame loss.

Chapter 6

Conclusion

The 802.21 framework for the simulation in the Network Simulator 3 has been performed. It shows the overall optimization in a vertical handover. The 802.21 framework not only includes the MIHF, but also the DHCP module, and the MIIS module. The use of an RDF Schema in the MIIS module is also important, since it allows retrieving information about near Points of Access in the proximity of the Mobile Node.

6.1 Results

The vertical handover time is the expected result from the simulation. It shows the difference between handover times, when a handover is performed with MIHF, or without MIHF. The difference between both is great, varying from a few mili-seconds to a few hundred mili-seconds. It also shows that is possible to perform a seamless handover with MIHF, in opposition to the handover without MIHF.

6.1.1 Handover Time without MIHF

The value expected to an handover time without MIHF is comprised of the time spent to perform a scanning, to associate, to authenticate and to configure the IP parameters by the Mobile Node. As could be seen, the most important value is the scanning time, which takes about 600 ms. This value is too great to perform a seamless handover, and will probably alert the Mobile Node's user that a handover is being made. The experiences confirm and validate this value, making the time taken to perform the other processes, insignificant, in comparison with the handover time.

6.1.2 Handover Time with MIHF

Using MIHF and the information provided by a SPARQL query made, it is possible to know the Wifi channel and the SSID of the Wifi PoA before the handover is made. This makes the handover times small, in comparison with the values seen in the previous section. Considering that the handover made is a make – before – break handover, the result as a seamless handover makes it undetected by the Mobile Node's user. The handover times are expected, since it takes not only the time to perform the handover, seen by the Round Trip Time of the DHCP frames, but also takes the time for the UMTS PoA to end transmitting packets from its queue.

6.2 Future Work

This work comprises the 802.21 framework to perform handover. It also demonstrates the use of a Media Independent Handover Function to perform a handover from a UMTS link to a Wifi link. Assuming that the Wifi link will be improved, so that the Wifi NetDevice is able to monitor packet loss and hence, generate MIHF LinkGoingDown events; it may be possible to detect and perform a handover between two Wifi links, or even from a Wifi link to an UMTS link.

The new 802.16 module, still in its development phase, may also be adapted to implement and improve a handover between this mobile network and one of the already implemented technologies, the UMTS or the Wifi.

In the course of the work, some MIHF primitives were not necessary. This primitives, such as the ones responsible for the remote registration of events, could be developed in a later scope.

References

[1] 1. **Stein, J.** Survey of IEEE802.21 Media Independent Handover Services. November 2006.

[2] 2. IEEE P802.21/D01.09, Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services. September 2006.

[3] 3. **Perkins, C.** Mobile IP. May 1997.

[4] 4. —. IP Mobility Support. 1996.

[5] 5. ANSI/IEEE Std 802.11 . 1999.

[6] 6. **Brenner, P.** A Technical Tutorial on the IEEE 802.11 Protocol. 1997.

[7] 7. IEEE Std 802.11e. 2005.

[8] 8. IEEE P802.11k/D5.0. 2006.

[9] 9. **S. Bangolae, C. Bell, E. Qi.** Performance Study of Fast BSS Transition using IEEE 802.11r. July 2005.

[10] 10. IEEE Std 802.16. 2004.

[11] 11. IEEE Std 802.16e. 2005.

[12] 12. **T. Ojanpera, R. Prasad.** An Overview of Air Interface Multiple Access for IMT-2000/UMTS.

[13] 13. **Nielen, M. van.** UMTS: A Third Generation Mobile System. 1992.

[14] 14. **A. Dutta, S. Das, D. Famolari, T. Ohba, K. Taniuchi, T. Kodama, H. Schulzrinne.** Seamless Handover across Heterogeneous Networks – An IEEE 802.21 Centric Approach.

[15] 15. **Q. Mussabbir, W. Yao.** Optimized FMIPv6 Handover using IEEE802.21 MIH Services. December 2006.

[16] 16. NS-3 Tutorial. 2008.

[17] 17. **Q. Mussabbir, W. Yao, Z. Niu, X. Fu.** Optimized FMIPv6 using 802.21 MIH Services in Vehicular Networks. February 2007.

[18] 18. **Gupta, V.** IEEE P802.21 Tutorial. July 2006.

[19] 19. **G. Di Caro, S. Giordano, M. Kulig, D. Lenzarini, A. Puiatti, F. Schwitter.** A Cross-Layering and Autonomic Approach to Optimized Seamless Handover.

[20] 20. **T. Melia, D. Corujo, A. de la Oliva, A. Vidal, R. Aguiar, I. Soto.** Impact of heterogeneous network controlled handovers on multi-node mobile device design. *2007.*

[21] 21. **F. Teraoka, K. Gogo, K. Mitsuya, R.Shibui, K. Mitani.** Unified L2 Abstractions for L3-Driven Fast Handover. November 2006.

[22] 22. **N. A. Fikouras, K.El Malki, S. R. Cvetkovic, C. S,ythe.** Performance of TCP and UDP during Mobile IP Handoffs in Single-Agent Subnetworks. 1999.

[23] 23. **I.Ramani, Stefan Savage.** SyncScan: Pratical Fast Handover for 802.11 Infrastructure Networks.

[24] 24. **S. Mangold, L. Berlemann.** IEEE 802.11k: Improving Confidence in Radio Resource Measurements. 2005.

[25] 25. IEEE P802.11r/D4.0. 2006.

[26] 26. **S. Choi, G. Hwang, T. Kwon, A. Lim, D. Cho.** Fast Handover Scheme for Real-Time Downlink Services in IEEE 802.16e BWA System. 2005.

[27] 27. **Rapeli, J.** UMTS: Targets, System Concept, and Standardization in a Global Framework. 1995.

[28] 28. **J. Dai, L. Chiang.** A New Method to Detect Abnormal IP Address on DHCP. 2007.

[29] 29. **R. Droms.** Automated Configuration of TCP/IP with DHCP. 1999.

[30] 30. **C. Park, S. Ahn, J.Chung.** The Improvement for Integrity between DHCP and DNS. 1997.

[31] 31. **R. Pereira, M. Freire.** SWedt: A Semantic Editor Integrating Ontologies and Semantic Annotations with Resource Description Framework. 2006.

[32] 32. **C. Laborda, S. Conrad.** Bringing Relational Data into the SemanticWeb using SPARQL and Relational.OWL. 2006.

[33] 33. **E. P. Shironoshita, Y. Jean-Mary, R. Braddley, M. Kabuka.** semQA: SPARQL with Idempotent Disjunction. February 2008.

[34] 34. **A. Langegger, M. Blochl, W. Wob.** Sharing Data on the Grid using Ontologies and distributed SPARQL Queries. 2007.

[35] 35. **Y. Kim, B. Kim, H. Lim.** The Index Organizations for RDF and RDF Schema. February 2006.