Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2008

Hugo Miguel Leonardo Proença

Avaliação de WiMAX para comunicações em aplicações de tráfego

Evaluating WiMAX for real-time vehicular communications

Hugo Miguel Leonardo Proença

Avaliação de WiMAX para comunicações em aplicações de tráfego

Evaluating WiMAX for real-time vehicular communications

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de mestre em Eng. Electrónica e Telecomunicações, realizada sob a orientação científica de José Alberto Fonseca e João Nuno Pimentel da Silva Matos, Doutores do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

O Júri / The Jury

Presidente

Doutor Valeri Skliarov
Professor Catedrático da Universidade de Aveiro

Vogais

Doutor José Alberto Gouveia Fonseca (Orientador)
Professor Associado da Universidade de Aveiro

Doutor João Nuno Pimentel da Silva Matos (Co-orientador)
Professor Associado da Universidade de Aveiro

Doutor Luis Miguel Moreira Lino Ferreira
Professor Equiparado a Professor Adjunto do Departamento de Engenharia Informática do Instituto Superior de Engenharia do Porto

agradecimentos / acknowledgements

Expresso desta forma a minha gratidão para com o meu orientador, Doutor José Alberto Fonseca e co-orientador, Doutor João Nuno Pimentel da Silva Matos por toda a ajuda prestada durante a realização deste trabalho.
Queria agradecer em especial ao meu companheiro de trabalho, André Amaral Costa, que com a sua ajuda e cooperação permitiu uma melhor realização desta dissertação.
Um outro agradecimento especial vai para o Doutor Paulo Bacelar Reis Pedreiras, que contribuiu bastante para os resultados obtidos neste trabalho.
Queria expressar a minha gratidão para com o Eng. Álvaro Gomes, devido à sua inteira disponibilidade para ajudar, e para com o meu colega de trabalho Miguel Pereira.
Aproveito também esta oportunidade para agradecer as pessoas que me são mais próximas, aos meus pais, Francisco e Maria, ao meu irmão, Jorge, e minha namorada, Helena, por todo o apoio que me têm dado ao longo do meu percurso académico.

Resumo

Os acidentes rodoviários têm um impacto elevado na sociedade, quer devido às perdas humanas daí resultantes quer devido aos custos económicos associados. Este facto tem causado por todo o mundo o estudo de mecanismos que permitam aumentar a segurança rodoviária. Um exemplo disto é o investimento da Europa em vários projectos com vista a desenvolver estes mecanismos, onde a maior parte destas iniciativas consideram a possibilidade dos veículos comunicarem entre si e/ou com estações fixas, situadas junto da rodovia. A mobilidade dos veículos apresenta requisitos especiais, onde as comunicações sem-fios têm um papel crucial nestas aplicações. Contudo, os serviços de segurança rodoviária requerem alguns requisitos específicos, como largura de banda ou em termos de *timeliness*, que têm de ser cumpridos independentemente da tecnologia sem-fios usada. Neste trabalho é pretendido avaliar WiMAX para comunicações relacionadas com a segurança rodoviária, em que a coexistência de diferentes tipos de serviços é uma realidade, onde o uso dos mecanismos de qualidade de serviço fornecidos pelo WiMAX podem ser uma vantagem.

Abstract

Road accidents have a huge impact on the society, both because of the resulting human life losses and injuries as well as because of the associated economic costs. This situation fostered the study of mechanisms for increasing road safety all over the world. In Europe, several projects are being funded to develop such mechanisms. Many of the approaches that are being pursued require the ability of the vehicles to communicate with each other and/or with fixed roadside equipments. Due to the mobility constraints, wireless technologies have a crucial role in this kind of applications. However, road safety services have also specific demands, in terms of bandwidth and timeliness, that have to be met, independently of the wireless technology used. In this work, it is performed an evaluation of WiMAX for road safety communications, taking into consideration the coexistence of different types of service and that the use of quality of service mechanisms in this wireless technology could be an advantage.

Contents

List of Figures

List of Tables

Acronyms

ABS	Anti-lock Breaking System.
ADC	analog-to-digital converter.
AES	Advanced Encryption Standard.
AFC	Automatic Frequency Control.
AGC	Automatic Gain Control.
AK	authorization key.
AMC	Adaptative Modulation and Conding.
API	Access Point Interface.
ARQ	automatic repeat request.
ASIC	Application-Specific Integrated Circuit.
ASP	Associative String Processor.
ASP	Active Server Pages.
ATM	Asynchonous Transfer Mode.
AWGN	Additive white Gaussian noise.
BE	Best Effort.
BlueTooth®	BlueTooth.
BS	base station.
BSP	Board Support Package.
BTC	block turbo code.
CBC	cipher block chaining.
CC	convolutional coding.
CDMA	code division multiple access.
CES	Consumer Electronics Show.
CGI	Common Gateway Interface.
CICAS	Cooperative Intersection Collision Avoidance Systems.
CID	connection identifier.
CINR	carrier to interference-plus-noise ratio.
CLI	Command Line Interface.

CP	cyclic prefix.
CPE	customer premises equipment.
CPS	Common Part Sublayer.
CRC	cyclic redundancy check.
CS	Convergence Sublayer.
CTC	convolutional turbo code.
DAA	Digest Access Authentication.
DAC	digital-to-analog converter.
DCD	downlink channel descriptor.
DDS	Direct Digital Synthesis.
DES	Data Encryptio Standard.
DHCP	Dynamic Host Configuration Protocol.
DIUC	downlink interval usage code.
DL	downlink.
DLFP	downlink frame prefix.
DMA	Direct Memory Access.
DSA	dynamic service addition.
DSRC	Dedicated Short Range Communications.
EAP	Extensible Authentication Protocol.
END	Enhanced Network Driver.
ertPS	extended real-time Polling Service.
ESP	Electronic Stability Program.
FCH	frame control header.
FDD	frequency division duplexing.
FEC	forward error correction.
FFT	fast Fourier transform.
FIFO	frist-in, frist-out.
FP6	Sixth Framework Program.
FP7	Seventh Research Framework Program.
FPs	Framework Programmes.
FTP	File Transfer Protocol.
GPIO	General Purpose Input/Output.
GPRS	General Packet Radio Service.
GSM	Global System for Mobile Communications.

H-FDD	half-duplex frequency division duplexing.
HARQ	Hybrid Automatic Repeat Request.
HCS	header check sequence.
HDTV	High-definition television.
HT	Header Type.
HTTP	Hypertext Transfer Protocol.
HUMAN	High-speed Unlicensed Metropolitan Area Network.
I2V	Infrastruct-to-Vehicle.
I^2C	Inter-Integrated Circuit.
ICMP	Internet Control Message Protocol.
IDU	Indoor Unit.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
IF	Intermediate Frequency.
IFFT	inverse fast Fourier transform.
IP	Internet Protocol.
ISI	intersymbol interference.
ITS	Intelligent Transportation System.
LDPCC	low-density parity check coding.
LLC	Logical Link Control.
LMAC	Lower MAC.
LOS	Line-of-Sight.
MAC	Medium Access Control layer.
MIB	Management Information Base.
MIMO	multiple-input, multiple-output.
MPDU	MAC protocol data unit.
MS	Mobile Station.
MSDU	MAC service data unit.
MTU	Maximum Transmit Unit.
NLOS	non-line-of-sight.
NPT	Network Protocol Toolkit.
nrtPS	nonreal-time Polling Service.

OBU	On Board Unit.
ODU	Outoor Unit.
OFDM	Orthogonal Frequency Division Multiplexing.
OFDMA	Orthogonal Frequency Division Multiple Access.
OSI	Open System Interconnection.
PAPR	peak to average power ratio.
PCI-X	Peripheral Component Interconnect Extended.
PCs	personal computers.
PDU	Protocol Data Unit.
PHS	Payload Header Suppression.
PHSF	Payload Header Suppression Field.
PHSI	Payload Header Suppression Index.
PHSM	Payload Header Suppression Mask.
PHSS	Payload Header Suppression Size.
PHSV	Payload Header Suppression Valid.
PHY	Physical Layer.
PKM	Privacy Key Management.
PMP	point-to-multipoint.
PoE	Power over Ethernet.
PSAP	PHY Service Access Point.
PtP	point-to-point.
PUSC	Partial Usage of Subchannels.
QoS	quality of service.
RCC	regional control center.
RF	radio frequency.
RISC	Reduced Instruction Set Computers.
RITA	Research and Innovative Technology Administration.
RS-CC	Reed-Solomon concatenated with convolutional coding.
RSSI	received signal strength indicator.
RSU	road side unit.
RTOS	Real-Time Operating System.
rtPS	real-time Polling Service.
RTT	round trip time.
SA	security association.

SC	single carrier.
SDRAM	Synchronous Dynamic Random Access Memory.
SDU	service data unit.
SFID	service flow identifier.
SNMP	Simple Network Management Protocol.
SNR	signal-to-noise ratio.
SoC	System-on-Chip.
SOFDMA	Scable Orthogonal Frequency Division Multiple Access.
SPI	Serial Peripheral Interface.
SS	subscriber station.
SSL	Secure Socket Layer.
SUIT	Scalable, Ultra-fast and Interoperable Interactive Television.
TCC	Traffic Control Center.
TCP	Tansmission Control Protocol.
TCS	Traction Control System.
TDD	time division duplexing.
TDM	time division multiplexing.
TEK	traffic encryption key.
TFTP	Trivial File Transfer Protocol.
UCD	uplink channel descriptor.
UDP	User Datagram Protocol.
UGS	Unsolicited Grant Service.
UIUC	uplink interval usage code.
UL	uplink.
UMAC	Upper MAC.
USA	United States of America.
USDOT	U.S. Department of Transportation.
V2I	Vehicle-to-Infrastruct.
V2V	Vehicle-to-Vehicle.
VCTCXO	Voltage Controlled Temperature Controlled Crystal Oscillator.
VLAN	virtual local area network.
VoIP	Voice over Internet Protocol.
VSC	virtual traffic control sub-centre.
Wi-Fi®	wireless fidelity.

WiMAX Worldwide Interoperability for Microwave Access.

XML eXtensible Markup Language.

Chapter 1

Introduction

1.1 Motivation

Nowadays, road safety is a mainstream topic in society all over the world. The number of car accidents in the Portuguese roads in 2006 reached 35,680 involving more than 47,000 people from which 850 were killed [daI07]. In the European context the numbers are shoking: in 2005 only, more than 40,000 people were killed in road accidents [eF08]. This scenario has a dramatic and unacceptable impact in terms of human life losses and injuries as well as in the global economy. Working in partnership with initiatives created to encourage a change in drivers behavior, the reduction of speed limits, etc., technical aids supporting active and dynamic prevention of car accidents are being considered as a decisive way of achieving a reduction on the road accidents as well as on its impact in terms of injuries and fatalities.

One of the approaches to ameliorate the road and traffic safety is to improve the sensing capabilities, allowing the drivers to be informed in advance of abnormal and potentially dangerous situations such as collisions, traffic jams, approach of emergency vehicles, etc. This scenario will become possible if drivers and vehicles could communicate with each other or/and with roadside base stations.

Therefore, one way of reducing road fatalities is to make vehicles capable of getting useful information from roadside infrastructures which lead us to the concepts of Vehicle-to-Infrastruct (V2I) and Infrastruct-to-Vehicle (I2V) communication. V2I and I2V communication are inherently mobile applications, thus wireless technologies play a crucial role in this type os transmission. Several wireless technologies, such as Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), wireless fidelity (Wi-Fi®), BlueTooth (BlueTooth®), Dedicated Short Range Communications (DSRC) [ETS08] and others can and have been explored to perform V2I communication. One of the technologies that was not yet adequately explored in this type of applications is Worldwide Interoperability for Microwave Access (WiMAX), which has promising features (e.g. range, bandwidth and real-time guarantees) for this kind of application.

WiMAX is a standard-based wireless technology that allows fixed and mobile access with non-line-of-sight (NLOS) reaching data rates of 40 Mbps in a 3Km to 10 Km cell, per channel [For08]. This technology allows to have access to quality of service (QoS) in the Medium

Access Control layer (MAC) layer and therefore it enables a more efficient management of QoS. As a result WiMAX it could be a useful technology for V2I communication. WiMAX also enables us to have a bidirectional communication with configurable percentage of transmit/receive time (in time division duplexing (TDD)).

1.2 Potential applications

Building systems that can allow V2I communication implies the knowledge of what kind of applications and requirements (bandwidth, timeless, ...) can be used to improve the road safety. So, there are several applications where V2I communication can be used for road safety [Har05]:

- **Safety Warning**: The driver could get messages about dangerous situations that he/she is about to face (e.g. accidents, traffic jams, approach of emergency vehicles, etc). This application demands time requirements very specific because the late delivery of a message can compromise the safety system. The bandwidth used by a message of this application is low. Bidirectional communication can be considered, allowing the vehicle to transmit also safety information.

- **Assisted Driving**: The driver could be helped and assisted in order to take the correct behavior when facing a potential dangerous situation. Like the application mentioned before, the timeliness requirements are very specific and also low bandwidth messages will be exchange.

- **Traffic Management**: The V2I communication could be used to avoid or solve traffic jams informing drivers not to go along the problematic areas. Although this is not so critical like the applications before, the information of traffic management must be delivered in an appropriated time. If not, it doesn´t make sense.

But not only road safety applications can be considered. When having the possibility to have communication between an infrastructure and a vehicle then additional information transmission, like regional information (restaurants, monuments, ...) or commercial multimedia applications (video, music, ...), must be considered.

1.3 Objectives

The main focus of this work is to evaluate WiMAX for vehicular communications, more specifically, in V2I and I2V scenarios. Throughout this work, a preliminary project of a communication system that allows to send data in real-time, from a fixed station to road vehicles is discussed. In this scenario it was taken into account a local cluster where the fixed station works like a WiMAX base station (BS) and the vehicles like WiMAX subscriber station (SS). It will be carried out a deeper study of the requirements and constrains of the vehicular communications and a temporal characterization of the WiMAX time parameters, specially for the establishment of the connectivity between the two entities (BS and SS).

In order to analyse the road safety services potentially implemented using WiMAX, an equipment developed at WiRia Project. The WiRia project aims to develop a commercial Fixed WiMAX SS (based on Institute of Electrical and Electronics Engineers (IEEE) 802.16-2004 standard [IEE04]). This project is funded by Telesal [TEL08] and has the participation of the portuguese company PT Inovação [PTI08], Institute of Telecommunication from Aveiro [oT08a] and the University of Aveiro [oA08]. For this work it will be also used a commercial and WiMAX FORUM [For08] certified BS and SS. Considering a scenario where the BS will be a road side unit (RSU) and the SS a On Board Unit (OBU) in a vehicle, some tests will be performed to evaluate the use of WiMAX in vehicular communication with critical time requirements.

This works involves the collaboration of several entities: University of Aveiro [oA08]; Institute of Telecommunication in Aveiro [oT08a]; PT Inovação [PTI08]; and BRISA [BRI08].

Related to this work, it was accepted for oral presentation in Controlo 2008 conference [AU08] a paper entitled "ASSESSING WIMAX FOR VEHICULAR COMMUNICATIONS".

1.4 Document Outline

This dissertation is organized in 8 chapters, including this introductory chapter (chapter 1) which describes the motivation and the main purpose of this work, and a closing chapter where final conclusions and a possible future line of work are presented (chapter 8).

Chapter 2 is entitled State-of-the-Art. In this, it will be presented a study of a set of European projects in the road safety area, with a reference about its objectives and the work that has been done. It is also given an overview of the usage of WiMAX in V2I communications.

In chapter 3 an overview of WiMAX technology is presented. Here, some technical aspects of this technology are described, more orientated for the MAC and Physical Layer (PHY).

In chapter 4 a study of WiMAX the Network Entry process is presented as well as an analysis of this process in V2I communications scenarios.

The chapter 5 presents a study of several of the available Fixed WiMAX development boards and systems, which could be potentially chosen to develop a WiMAX SS. It is also introduced the commercial equipments used in this work.

In chapter 6 the effort that was employed in order to transform a development board in a commercial SS is reported, presenting the features supplied by the development board and then the changes made and the drawbacks encountered.

Finally, chapter 7 presents an evaluation of available WiMAX equipments for road safety services. The requirements of these services are discussed and the WiMAX QoS mechanisms to accomplish them are evaluated.

Chapter 2

State-of-the-Art

2.1 Introduction

In the last decades, a substantial effort has been devoted to the study and development of mechanisms that could improve road safety, namely studies dedicated to in-vehicle subsystems that operate entirely based on local sensors and actuators: e.g. the Anti-lock Breaking System (ABS), which avoids the wheel skidding when the driver actuates the breaks; the Traction Control System (TCS), which prevents traction wheel skidding during acceleration; the Electronic Stability Program (ESP), which actively corrects the vehicle path according to the steering wheel input; etc. However, these mechanisms are merely reactive disabling us to foresee potentially dangerous situations. Despite being extremely useful, they exhibit a limited scope of coverage.

One way of overcoming this limitation is to develop the cooperation between vehicles and the infrastructure. A possible approach consists on using wireless communication among vehicles and/or between vehicles and the roadside infrastructure (figure 2.1), in order to transmit information. Consequently the drivers' radius of perception is effectively enlarged allowing him to becomes aware of potentially dangerous situations which can be anticipated and improving the driver's capability in carrying out correct maneuvers and avoiding accidents. These mechanisms have a major importance on many common but potentially dangerous daily road situations such as the report of accidents,the approach of traffic jams or other obstacles in highways, the approach of emergency vehicles, lane changes, the crossing of highway intersections, etc.

The European Commission and the automotive industry are strongly committed to improve road safety and to reduce the number of accidents in European roads. The initiative eSafety [eSa08] reflects this preoccupation: "eSafety, the first pillar of the Intelligent Car Initiative, is a joint initiative of the European Commission, industry and other stakeholders and aims to accelerate the development, deployment and use of Intelligent Integrated Safety Systems" in [eSa08]. The eSafety initiative is also associated to the eSafety Forum [eF08] whose aim is to promote and monitors the implementation of the recommendations identified by the eSafety Working Group, as well as supporting the development, deployment and use of new and intelligent integrated road safety systems. Since 2002, this initiative has funded a

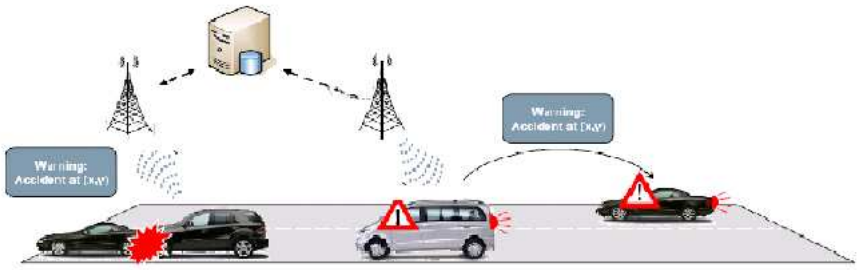

Figure 2.1: Coexistence of V2V and V2I communications, adapted from [Kar06]

number of projects, in some of which the Vehicle-to-Vehicle (V2V) and V2I communications played a significant role.

2.2 Brief survey of relevant safety related projects

The European Union is funding several projects that use information and communication technologies in intelligent solutions, in order to increase road safety [Ini08]. From 2002 to 2006, the projects were funding by the Sixth Framework Program (FP6) which has the objective to promote the scientific and technological bases of industry and encourage its international competitiveness while promoting research activities [Pro08b]. Nowadays, the Seventh Research Framework Program (FP7) is current financial tool support research and development activities in Europe [Pro08a]. The Framework Programmes (FPs) have been the main financial tools through which the European Union supports this activities covering almost all scientific disciplines. FPs are proposed by the European Commission and adopted by Council and the European Parliament following a co-decision procedure. The FP7 have a duration of seven years (from 1^{st} January 2007 to 31^{th} of December 2013) and has a total budget of over €50 billion.

2.2.1 COMeSAFETY

(FP6 funded with €1.1 million). The COMeSafety project [COM08c] supports the eSafety Forum with respect to all issues related to V2V and V2I communications as the basis for cooperative intelligent road transport systems. It is composed by a projects network 2.2 and the main objectives goals are:

- Co-ordination and consolidation of research results and their implementation
- eSafety Forum support in case of Standardisation and Frequency Allocation
- Worldwide harmonization (Japan/US/Europe)

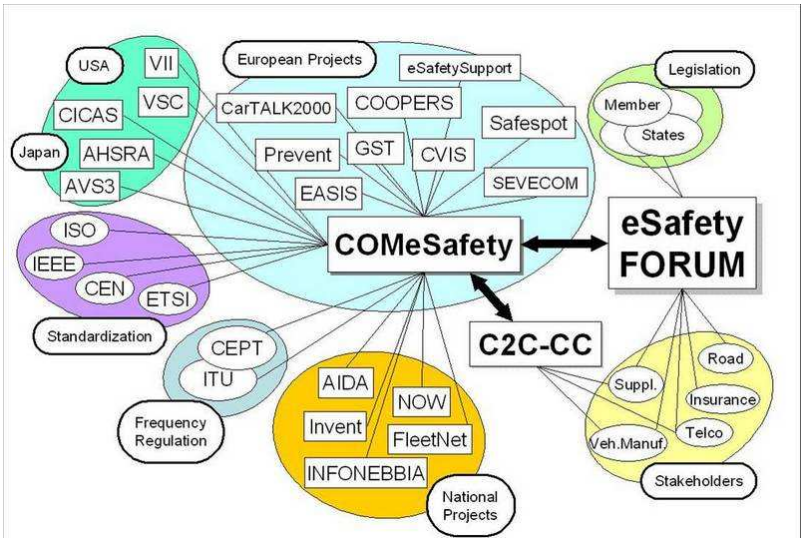

Figure 2.2: COMeSAFETY projects network, from [COM08c]

- Support Frequency allocation process
- Dissemination of the results

2.2.2 COM2REACT

(FP6 funded with €3.0 million). The vision of the COM2REACT [COM08a] project is to create a three level architecture in order to improve road efficiency and safety: a low level control that is done inside each vehicle; a middle level control provided by a local center to the vehicles in the area; and a high level control of a metropolitan or urban area provided by a regional center [COM08a]. The main feature of COM2REACT is a virtual traffic control sub-centre (VSC), which controls a moving group of vehicles in close proximity (medium level). This VSC will be inside a car that is moving and uses V2V communication to send and receive information providing safety instructions to the vehicles that are in its vicinity (figure 2.3). The VSC uses V2I communication to send traffic related information to the regional control center (RCC) and also receives from it some data to send to the vehicles that are on the area. It is also wanted to adapt existing communication technologies to perform these communications (ex. Wi-Fi®, GPRS) [COM08a].

2.2.3 COOPERS

(FP6 funded with 9.8M€). The ambition of the COOPERS [COO08] project is to connect vehicles to road infrastructures on motorways (figure 2.4). This link will allow the exchange of data and information to increase the safety in specific road segments. The mission is to define and develop services and equipment to provide bi-directional links between the V2I using an open standardized wireless communication technology. A stable link needs to be established in

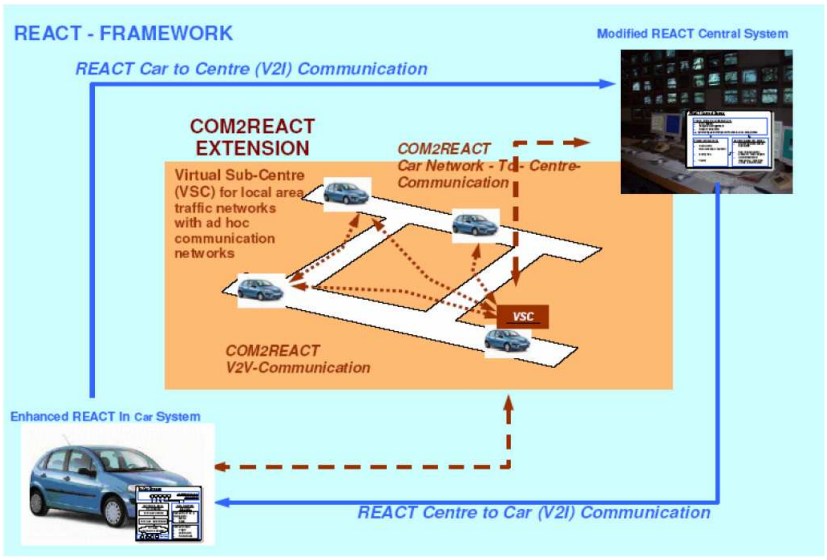

Figure 2.3: COM2REACT VSC communication, from [COM08b]

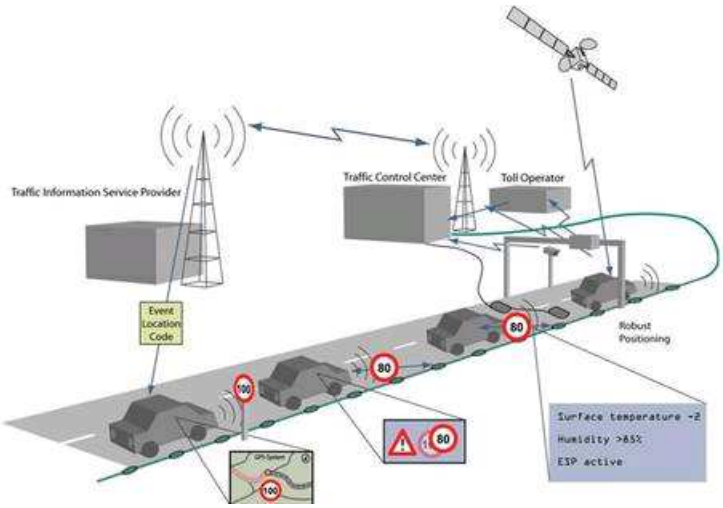

Figure 2.4: COOPERS vision, from [COO08]

---

order to ensure the transmission of real-time location-based safety related information on the current traffic status [COO08]. The highest effect of V2I communications will be achieved in areas of dense traffic, where the risk of accidents and traffic jams is extremely high [COO08].

2.2.4 CVIS

(FP6 funded with 21.91M€). The Cooperative Vehicle-Infrastructure Systems [CVI08a] has the main objective of creating standardized in-vehicle and roadside modules capable of communicate continuously and seamlessly using a wide range of communication media,

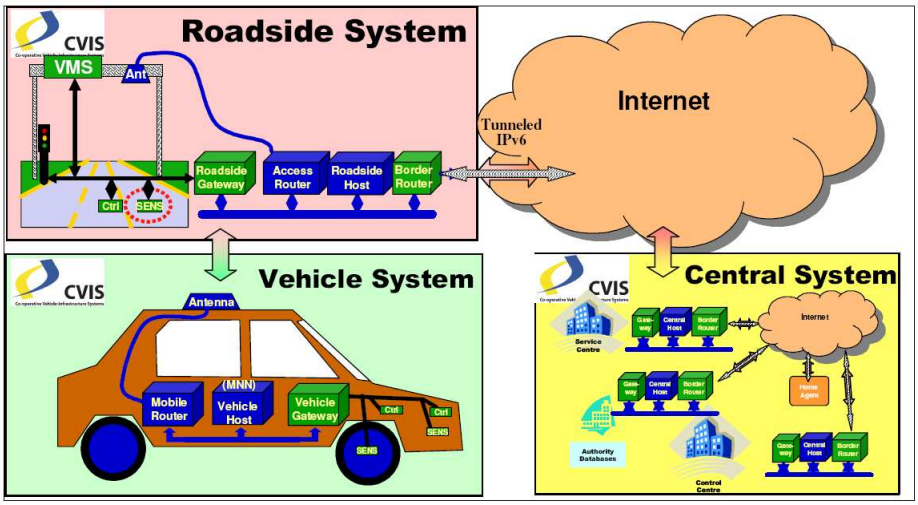

Figure 2.5: CVIS communication concept, from [CVI08b]

---

including mobile cellular and wireless local area networks, short-range microwave (DSRC) or infrared. It is also the intent of this project to develop techniques for better vehicle localization and improved local dynamic maps, using for that satellite navigation and state-of-the-art methods for localization referencing. Define and test new systems for cooperative traffic and network monitoring, to use both in vehicle and roadside equipment, as well as detecting incidents instantly and anywhere, are also objectives of [CVI08a]. In figure 2.5 is represent the high level architecture of CVIS project.

2.2.5 SAFESPOT

(FP6 funded with 20.59M€). The SAFESPOT [SAF08] proposes an open, flexible and modular architecture and communication platform, where both the infrastructure and the vehicles are sources and destinations of safety-related information. The project also aims at develop a new generation of infrastructure-based sensing techniques. There were defined two types of test scenarios:

1. Static black spots or "static risky conditions", which are road scenarios intrinsically dangerous, statistically identifiable, such as narrow curves, tunnels and bridges;

2. Dynamic black spots or "dynamic risky conditions", which are where the driving scenarios may become unexpectedly and suddenly dangerous.

The technological challenges faced by this project are the availability of a reliable, fast, secure and potentially low cost protocol for local vehicle to vehicle and vehicle to infrastructure communication. A possible candidate is the radio technology, currently under standardization, IEEE 802.11p.

2.3 Others projects in the world

In the United States of America (USA), the Research and Innovative Technology Administration (RITA) coordinates the U.S. Department of Transportation (USDOT) research programs which have the objective of deployment of cross-cutting technologies to improve the transportation system, here safety is a priority [oT08b]. There are several initiatives that aims to improve the road safety, like the Cooperative Intersection Collision Avoidance Systems (CICAS) [Sys08] which pretends to warn drivers about likely violations of traffic control devices and to help them maneuver through cross traffic, using build-in vehicle devices (e.g., sensors), Infrastructure-based technologies and systems (e.g., roadside sensors) and communication systems (e.g., DSRC communications for I2V communications).

Japan shows the motivation in improve the road safety mainly through the Intelligent Transportation System (ITS) initiative. One example of that is demonstrations like "Smartway 2007 Demo" [20008] here was mount a test ride in a Tokyo Metropolitan Expressway in order to test different types of systems to improve the road safety. In this demonstration, 60 cars equipped with an OBU were made available to 666 people to experience (and test) the road safety equipments benefits.

2.4 WiMAX usage in vehicular communications

WiMAX technology is being considered for usage in I2V communication, but not mainly in a road safety environment. There are several projects/demonstrations where WiMAX is used for supply broadband services between an infrastructure and a vehicle. One example of that is the demonstration that Intel [INT08] presents during the Consumer Electronics Show (CES) 2008 (in Las Vegas) [Sho08]: a full working demonstration of a IEEE 802.16e-2005 network. One demonstration performed was to have a videoconference in vehicle at 45 miles per hour, having also multiple hand-offs between the base stations. It was possible to a have 3Mbps in downlink and a 1.5Mbps in uplink, using 2.6 GHz for central frequency in a 3 sectors BS.

In order to develop a Mobile WiMAX in-vehicle navigation system, Oki Electric Industry, Co., Ltd. [OEI08], Alpine Electronics Inc [Inc08], and Runcom Technologies Ltd. [Ltd08] join forces to build first car navigation system with streaming content based on Mobile WiMAX technology.

One project that is testing WiMAX for exchange information in a I2V communication is Scalable, Ultra-fast and Interoperable Interactive Television (SUIT) [Pro08c], which objective is to explore several techniques to minimize the mixing the internet protocol and a broadcasting network and make it available to mobile users moving at high speed. Wireless technologies that are being explored in this project are DVB-T/H and WiMAX. In recent publication [Pla08], it was show that is possible to spread High-definition television (HDTV) through WiMAX moving at 140 Km.

In a road safety environment, the European project COOPERS [COO08] consider the use of WiMAX as a backhaul technology, for example, to transport information between a RSU and a central management point (Traffic Control Center (TCC)).

2.5 Conclusions

The projects previously presented prove the effort that has been done to intensify road safety. The dramatic impact that road accidents have on the society is fostering the research of mechanisms to increase road safety all over the world. Most of the approaches that have been developed depend on the ability of the vehicles to communicate with each other and/or with fixed roadside equipments.

There is no wireless technology defined as being the most appropriate one for V2I and I2V communications. In some projects, the use of standard based technologies such as GSM or Wi-Fi® is already being applied. However, some of them are taking into consideration the improvement of the existent standards which can lead to the appearance of new technologies, such as DSRC [ETS08], where PHY and MAC come from a standard family, the IEEE 802.11p, which is totally orientated for vehicular communications, specially for road safety issues.

It is possible to consider exploring the WiMAX technology for vehicular communications. Although WiMAX is a recent technology, it has been proved that it is possible to use it to supply V2I and I2V communication. Road safety communications have some requirements that need further study that can be matched in the WiMAX technology.

Chapter 3

WiMAX Technology

3.1 Introduction/Background

The IEEE 802.16 [IEE08] group was formed in 1998 to develop an air-interface standard for wireless broadband [JGA06]. This group's initial purpose was the development of a Line-of-Sight (LOS)-based point-to-multipoint (PMP) wireless broadband system for operation in the 10GHz-66GHz, which resulted in the original 802.16 standard, published in December 2001. This standard was based on a single-carrier PHY layer with a burst time division multiplexing (TDM) MAC layer. Subsequently, the IEEE 802.16 group produced the 802.16a amendment, to include NLOS applications in the 2GHz-11GHz band, using an Orthogonal Frequency Division Multiplexing (OFDM)-based physical layer. In 2004, a new standard called IEEE 802.16-2004 [IEE04], replaced all prior versions and formed the basis for the first Fixed WiMAX solution [Pap08b]. In December 2005, the IEEE group completed and approved IEEE 802.16e-2005 [IEE05b], an amendment to the IEEE 802.16-2004 standard that added mobility support and forming the basis for the Mobile WiMAX [Pap08a]. The WiMAX Forum [For08] is an industry-led, non-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard. A WiMAX Forum goal is to accelerate the introduction of these systems into the marketplace [Pap08b]. The WiMAX forum has also established some profiles for certification (figure 3.1). There are profiles for Fixed WiMAX and for Mobile WiMAX. Each profile sets well defined values for the frequency, channel bandwidth, OFDM fast Fourier transform (FFT) size and duplexing, to allow equipments from different manufacturers to work together, under the condition of respecting the same profile achieving interoperability.

3.2 Key Features

Like was mentioned before, the WiMAX Forum defines two different versions: Fixed and Mobile WiMAX; where both are based on the IEEE 802.16 group standards. Below are presented some of key features of the WiMAX as wireless technology [CE06] [JGA06]:

Band Index	Frequency Band	Channel Bandwidth	OFDM FFT Size	Duplexing	Notes
Fixed WiMAX Profiles					
1	3.5 GHz	3.5MHz	256	FDD	Products already certified
		3.5MHz	256	TDD	
		7MHz	256	FDD	
		7MHz	256	TDD	
2	5.8GHz	10MHz	256	TDD	
Mobile WiMAX Profiles					
1	2.3GHz–2.4GHz	5MHz	512	TDD	Both bandwidths must be supported by mobile station (MS)
		10MHz	1,024	TDD	
		8.75MHz	1,024	TDD	
2	2.305GHz–2.320GHz, 2.345GHz–2.360GHz	3.5MHz	512	TDD	
		5MHz	512	TDD	
		10MHz	1,024	TDD	
3	2.496GHz–2.69GHz	5MHz	512	TDD	Both bandwidths must be supported by mobile station (MS)
		10MHz	1,024	TDD	
4	3.3GHz–3.4GHz	5MHz	512	TDD	
		7MHz	1,024	TDD	
		10MHz	1,024	TDD	
5	3.4GHz–3.8GHz, 3.4GHz–3.6GHz, 3.6GHz–3.8GHz	5MHz	512	TDD	
		7MHz	1,024	TDD	
		10MHz	1,024	TDD	

Figure 3.1: Certifications Profiles defined by WiMAX Forum, from [JGA06]

- **OFDM-based PHY** - scheme that offers a robust behavior in presence of multipath radio signal propagation, allowing WiMAX to operate in NLOS conditions.

- **Very high peak data rates** - the peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum (in both directions, downlink and uplink).

- **Scalable bandwidth and data rate support** - a scalable PHY architecture that allows for the data rate to scale easily with the available channel bandwidth. This scalability is supported in the Orthogonal Frequency Division Multiple Access (OFDMA) mode, where the FFT size may be scaled based on the available channel bandwidth. This is not applicable for fixed WiMAX.

- **Adaptative Modulation and Conding (AMC)** - the WiMAX supports a number of modulation and forward error correction (FEC) coding schemes and allows the scheme to be changed on a per user and per frame basis, based on the instantaneous channel conditions. AMC is an effective mechanism to maximize throughput in a time-varying channel.

- **Link-layer retransmissions** - for connections that require enhanced reliability, WiMAX supports automatic repeat request (ARQ) at the link layer. ARQ-enabled connections

require each transmitted packet to be acknowledged by the receiver so unacknowledged packets are retransmitted. The Mobile WiMAX optionally supports Hybrid Automatic Repeat Request (HARQ), which is an effective hybrid between FEC and ARQ.

- **Support for TDD and frequency division duplexing (FDD)** - the WiMAX supports TDD, FDD and Half-FDD.

- **OFDMA** - Mobile WiMAX uses OFDM as a multiple-access technique, whereby different users can be granted with different subsets of OFDM tones. This is not applicable for fixed WiMAX.

- **Flexible and dynamic per user resource allocation** - both uplink (UL) and downlink (DL) resource allocation are controlled by a scheduler in the BS. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme. When using the OFDMA-PHY mode, multiplexing is additionally done in the frequency dimension, by allocating different subsets of OFDM subcarriers to different users. The IEEE 802.16 allows broadcast and multicast messages, which optimizes the use of the spectrum.

- **Support for advanced antenna techniques** - The WiMAX solution has a number of hooks built into the physical-layer design, which allows for the use of multiple-antenna techniques, such as beamforming, space-time coding, and spatial multiplexing. These schemes can be used to improve the overall system capacity and spectral efficiency by deploying multiple antennas at the transmitter and/or the receiver.

- **QoS support** - The WiMAX MAC layer has a connection-oriented architecture that is designed to support a variety of applications, including voice and multimedia services. The system offers support for constant bit rate, variable bit rate, real-time, and non-real-time traffic flows, in addition to best-effort data traffic.

- **Robust security** - WiMAX supports authentication and strong encryption and has a robust privacy and key-management protocol.

- **Support for mobility** - The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications. The system also has built-in support for power-saving mechanisms that extend the battery life of handheld subscriber devices. PHY enhancements, such as more frequent channel estimation, uplink sub channelization, and power control, are also specified in support of mobile applications.

- **IP-based architecture** The WiMAX Forum has defined a reference network architecture that is based on an all-Internet Protocol (IP) platform. All end-to-end services are delivered over an IP architecture relying on IP-based protocols for end-to-end transport, QoS, session management, security, and mobility.

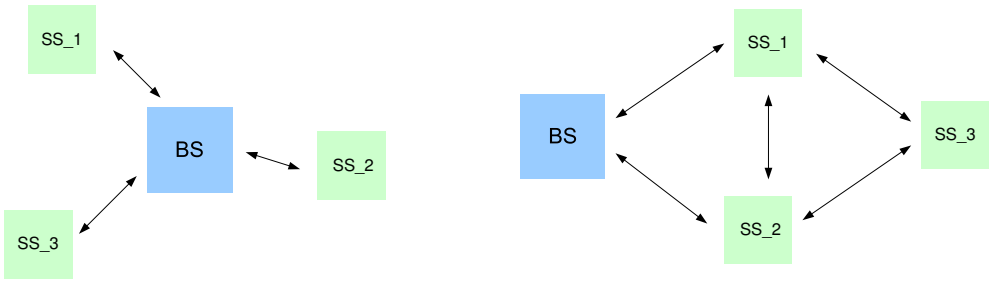

Figure 3.2: Point-to-Multipoint and Mesh topologies

3.3 Topology

The IEEE 802.16 defines two different topologies: PMP and Mesh [Nua07]. In the PMP topology (figure 3.2), the two logical entities, the BS and the SS[1], are in a master-slave relationship, where the SS must follow the medium access rules defined by the BS. In this topology, the SS only communicate with BS. On the other hand, in a Mesh topology SSs can route traffic from others SSs to the BS and traffic can be exchanged between SSs without passing in the BS (figure 3.2). In contrast of PMP topology, this is not a centralized system.

One of the basic differences between the BS and SS in a PMP configuration is that the BS, which acts as a centralized controller and a centralized distribution/aggregation point, has to coordinate transmissions to/from multiple SSs, whereas the SS need to deal with only one BS [CE06]. All traffic originating from an SS, including all SS-to-SS traffic, must go through the BS. Therefore, in a typically IEEE 802.16 system, the BS has to have additional processing and buffering capability (compared to a typical SS) to support a reasonable number of SSs.

The IEEE 802.16 mesh also includes the notion of BS and SS. However, the functionalities of these logical entities in mesh mode are sightly different from those of the BS and SS in PMP. Mesh topology is not yet part of a WiMAX certification profile.

3.4 IEEE 802.16 Reference Model

The IEEE 802.16 standard describes both the MAC and PHY for fixed and mobile WiMAX systems [CE06]. There are two major components of the wireless broadband system: the data/control plane and the management plane. The data plane defines how information is encapsulated or decapsulated in the MAC and modulated or demodulated by the PHY. A set of control function is needed to support various configuration and coordination functions. In the management plane is included the management of the classification, security, QoS, connection setup, and other functions. The IEEE 802.16 reference model is represented on figure 3.3. The IEEE 802.16 MAC of three major components called sublayers. The three

[1]In some configurations SS is referred to as the customer premises equipment (CPE) when that is physically located within the costumer's premises; The IEEE 802.16-2005 define the Mobile Station (MS) which requires additional SS specific functions such as mobility management, handoff, and power conservation.

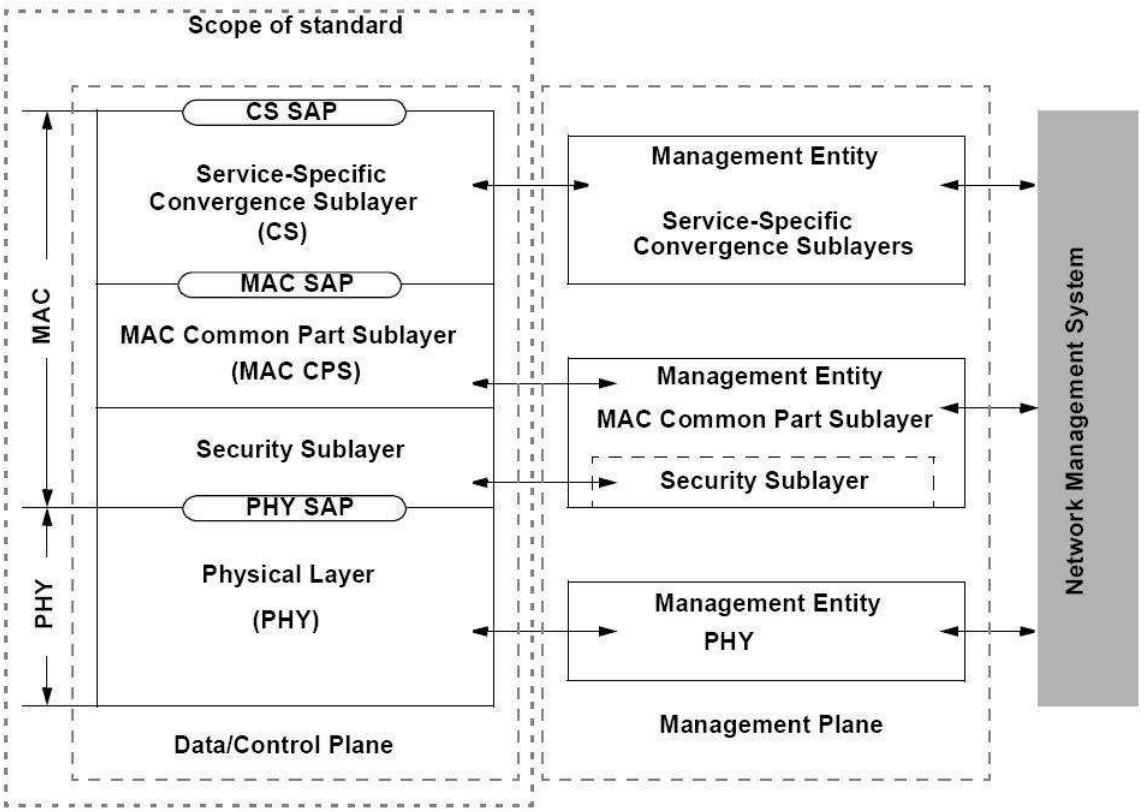

Figure 3.3: The IEEE 802.16 reference model, from [IEE04]

---

sublayers are service-specific Convergence Sublayer (CS), the MAC Common Part Sublayer (CPS), and the security sublayer.

To perform QoS at the MAC layer, the data unit, which come from upper layers (service data unit (SDU)), needs to be classified. A service-specific CS performs all functions that are specific to the higher layer protocol it supports, such as classification. IEEE 802.16 supports a set of CSs to interface with IP, Ethernet, and Asynchonous Transfer Mode (ATM) protocol layers. For WiMAX, only IP and Ethernet interface is considered.

The MAC CPS is responsible for performing the core MAC functions that are independent of the specific CS [CE06]. The MAC CPS receives MAC service data unit (MSDU) from the CS and transforms them into MAC protocol data unit (MPDU). The MAC CPS provides the medium access, connection management and QoS functions. The security sublayer is responsible for providing encryption, decryption, authentication, and secure key exchange functions.

The MAC CPS interfaces with the PHY through the PHY Service Access Point (PSAP). The MAC CPS may receive MSDUs from multiple MAC CSs. . It should be noted that the PSAP scheduling and allocation of bandwidth at the MAC CPS depends on the specific PHY type and parameters, although the MAC itself is PHY independent.

The management plane, represented in figure 3.3 consists of four management entities

corresponding to the CS, CPS, security sublayer, and the PHY. The IEEE 802.16 standard does not define the details of the management plane and it is outside the scope of IEEE 802.16. However, specific interfaces and messaging may be standardized to support management functions and an IEEE 802.16 amendment. The approved IEEE 802.16f amendment [IEE05a] defines a Management Information Base (MIB) for the fixed wireless access systems. Some of the MAC and PHY control messages currently defined in IEEE 802.16 may also be used to manage IEEE 802.16 systems through an external management system.

3.5 IEEE 802.16 MAC

The MAC function is responsible for controlling access to the medium. MAC is responsible for basic functions such as data encapsulation, fragmentation and adaptive modulation support. MAC define how MPDU errors are detected and how, if necessary, the faulty MPDUs are retransmitted. QoS and security are functions supported by MAC. The MAC, along with the Logical Link Control (LLC), is Layer 2 of the Open System Interconnection (OSI) reference model [CE06].

3.5.1 Convergence Sublayer

The CS enables the transparent transport of data from other protocol specification, e.g., ATM, Ethernet, or IP, over an IEEE 802.16 link in a transparent way. The CS hides the details of the payload protocol from the IEEE 802.16 MAC. Multiple CSs can coexist simultaneously, sharing the same MAC.

The CS receive SDUs from higher layers and map this SDUs to appropriate MAC service flow. Then, is responsible to deliver the processed packet to the MAC CPS for transmission. Optionally, before the deliver of Protocol Data Unit (PDU)s to CPS, CS can compress redundant payload protocol headers (Payload Header Suppression (PHS)). On other way, the CS receive the MAC CPS PDUs, restore any compressed payload protocol headers and deliver the payload protocol PDU to the higher layer.

The payload protocol PDU is mapped to the service by a set of configured rules called classifiers. The information a classifier considers depends on the protocol being transported. In the case of Ethernet and IP, it is possible to aggregate frames or packets to the same service flow for transport over the air in the CS.

The IEEE 802.16-2004 [IEE04] defines to types of CS:

- ATM CS - not used in current profiles of WiMAX;
- Packet CS.

Packet Convergence Sublayer

The Packet CS is designed to cope with any protocol utilizing packets for transporting data. Currently, the service flow signalling used for setting up the Packet CS supports only Ethernet and IP. The Packet CS PDU is represented in figure 3.4. Note that the Payload

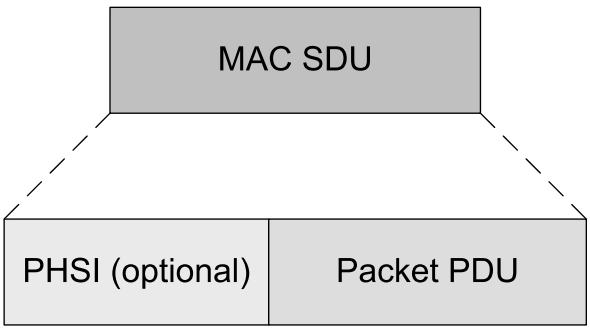

Figure 3.4: Packet Convergence Layer SDU format

Header Suppression Index (PHSI) field is always added when carrying Ethernet or IP, regardless of whether PHS is enabled for the connection. If PHS is used, the PHSI field indicates which PHS rule is to be applied by the receiver.

The Packet CS contains a classification function that determines on which MAC connection (with a respective connection identifier (CID)) a particular packet shall be carried and which PHS rule applies for that packet. In figure 3.5 is represent this process. The exact rules of classification and the parameters by which the classifier is configured depends on the upper layer protocol and its design. Classifier parameters are configured during dynamic service signalling. Each classifier rule is also associated with a priority. Rules with a higher priority take precedence.

If PHS is on, the BS and the SS negotiate the PHS parameters constituting a PHS rule. The PHS rule to be applied is determined by the sender based on the classification established in the Packet CS. The receiver, by inspecting the PHSI field, can determine the rule that was used to suppress a particular Packet CS PDU. The PHS parameters are [CE06]:

- PHSI: The index to the PHS rule.
- Payload Header Suppression Field (PHSF): A string of bytes containing the information allowing the receiver to reconstruct the suppressed information.
- Payload Header Suppression Mask (PHSM): A string of bits, each corresponding to a byte in the PHSF. If a bit is set, the corresponding byte is suppressed in the sender, and the receiver will reconstructed the byte based on the content of the PHSF.
- Payload Header Suppression Size (PHSS): A parameter indicating the local number of bytes to be processed by PHS. The value is always equal to the length (in bytes) of the PHSF.
- Payload Header Suppression Valid (PHSV): A boolean value indicating whether the sender will compare the actual packet header with the version as it will be reconstructed

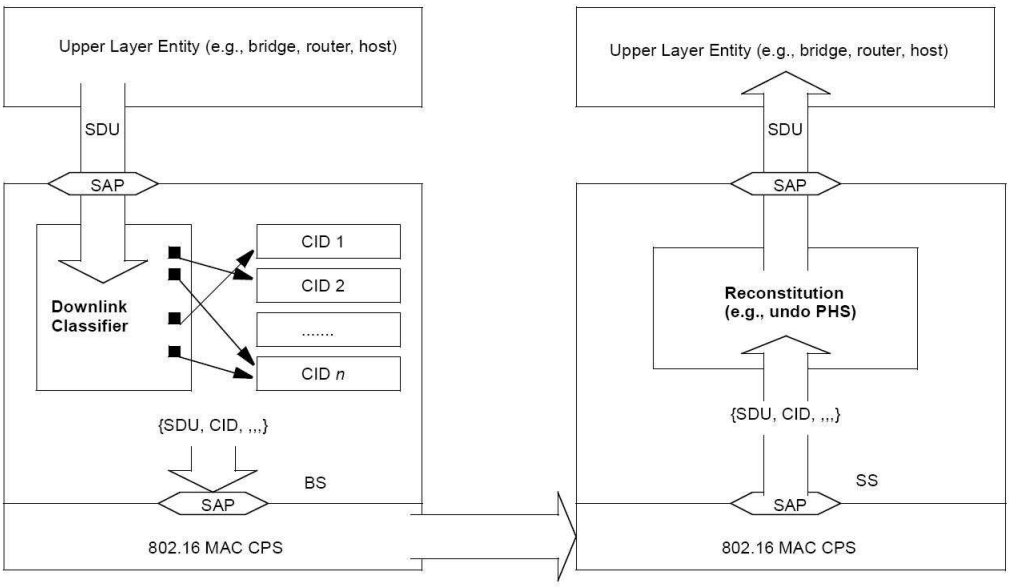

Figure 3.5: Classification and CID mapping (BS to SS), from [IEE04]

by the receiver. If the two don't match exactly, the headers of the higher layer are not suppressed, and the PHSI field in the Packet CS PDU is set to zero.

3.5.2 Common Part Sublayer

The IEEE 802.16 MAC CPS is independent of the higher-layer protocol and performs the scheduling, ARQ, bandwidth allocations, modulation, and code rate selection. Each air interface in SS shall have a 48-bit universal MAC address (as defined in IEEE 802-2001) [IEE05b]. This address uniquely defines the air interface of the SS from within the set of all possible vendors and equipment types. It is used during the initial ranging process to establish the appropriate connections for an SS. However, this MAC address is used to uniquely identify an SS only during initial registration or authentication and as part of some management messages.

The IEEE 802.16 MAC is connection oriented and identifies a logical connection between the BS and the SS by a unidirectional 16-bits CID. The CID can be viewed as a temporary and dynamic layer 2 address assigned by the BS to identify a unidirectional connection between the peer MAC/PHY entities and is used for carrying data and control plane traffic. At SS initialization, two pairs of management connections (two in the uplink and two in the downlink) shall be established between the SS and the BS and a third pair of management connections may be optionally generated. The **basic connection** (mandatory) is used by the BS MAC and SS MAC to exchange short, time-urgent MAC management messages [IEE04]. The **primary management connection** (mandatory) is used by the BS MAC and SS MAC to exchange longer, more delay-tolerant MAC management messages [IEE04]. The **secondary management connection** (optional), which is only required for a required

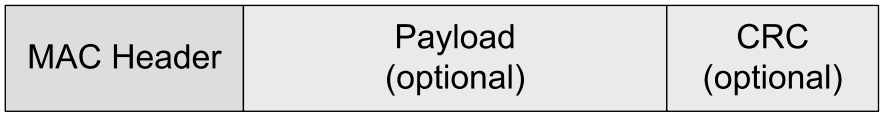

Figure 3.6: MAC PDU format

---

only for managed SS[2], is used by the BS and SS to transfer delay tolerant, standards-based messages (e.g. DHCP, Simple Network Management Protocol (SNMP), Trivial File Transfer Protocol (TFTP), etc.).

Service flows are used by the IEEE 802.16 MAC to efficiently support per-connection services such as QoS. A service flow is a MAC transport service that provides unidirectional transport of packets on the DL or on the UL. It is identified by a 32-bit service flow identifier (SFID) and each one have an associated CID.

MAC PDU Construction and Transmission

The IEEE 802.16 MPDUs (figure 3.6) are the units of data build by the MAC to the PHY for transmission and the unit of data delivered by the PHY to the MAC in the receiver. There are two classes of IEEE 802.16 MAC information transported between peer entities [CE06]: stand-alone MAC headers and MPDUs. The stand-alone header is the smallest possible information unit that can be transported between two nodes (6-bytes size).

Stand-alone MAC headers Stand-alone MAC headers are used to transport compact control or signalling information between an SS and a BS [CE06]. None of the stand-alone headers can be used to encapsulate any payload, as they are self-contained and used for a specific purpose. All currently defined stand-alone MAC headers are relevant only in the UL. A Header Type (HT) field is used to indicate whether the header is a generic MAC header (HT=0) or one of the stand-alone headers (HT=1). Additional fields, such as the Type field, are used to further distinguish the type of generic or stand-alone header being transported or other information that may be present in the payload. One of the most important stand-alone MAC headers is the Bandwidth request header (figure 3.7), which carries a full Bandwidth request from an SS.

MPDUs The MPDUs is used for carrying data and MAC signaling messages. Each MPDU begins with a 6-byte generic MAC header (represented in figure 3.8), followed by the optional variable-size payload. The payload may consist of MAC subheaders, management messages, special payloads, MSDUs received from a CS, or padding information. Additional, there is define five subheaders that can be used in MPDUs payload field [JGA06]:

[2]A managed SS is an SS which have a dedicated channel for non-MAC management (e.g. get an air interface IP address by Dynamic Host Configuration Protocol (DHCP))

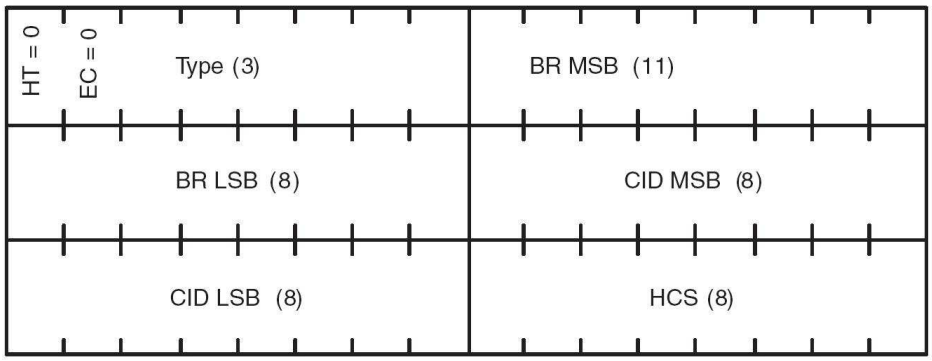

Figure 3.7: Bandwidth request header, from [JGA06]

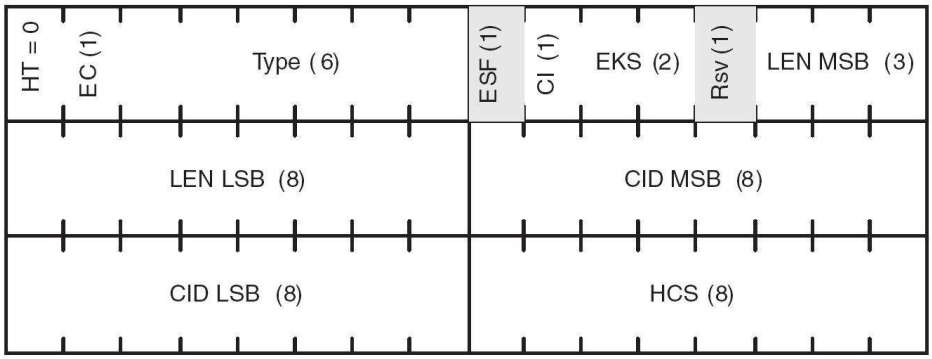

Figure 3.8: Generic MAC Header, from [JGA06]

---

1. *Grant-management subheader* - used by the SS for messages related to bandwidth management, such as polling request and additional-bandwidth request.
2. *Fragmentation subheader* - follows the generic MAC header and indicates that the SDU is fragmented over multiple MAC PDUs.
3. *Packing subheader* - indicates that multiple SDUs or SDU fragments are packed into a single MAC PDU and are placed at the beginning of each PHY SDU or PHY SDU fragment.
4. *Fast-feedback allocation subheader* - indicates that the PDU contains feedback from the SS about the DL channel state information.
5. *Mesh subheader*. Follows generic header when mesh networking is used.

Like is refereed in the subheaders enumeration, the MAC SDU can be fragmented in various MAC PDUs (**fragmentation**), or multiple SDUs can be aggregated in a single MAC PDU (**packing**). Additional, several MAC PDU can be transmitted in a single PHY burst (**concatenation**). For some of the IEEE 802.16 PHY specifications, an intermediate sublayer, called the transmission CS, is specified to efficiently support concatenation [CE06].

Transmitting over the air When the MAC PDU is constructed, it is handed over to the scheduler, which schedules the MAC PDU over the PHY resources available [JGA06]. It is checked the SFID and the CID of the MAC PDU, which allows to match it to the respective QoS requirements. The scheduling procedure is outside the scope of the IEEE 802.16 standard and has been left to the equipment manufacturers to implement[3].

Quality of Service

The IEEE 802.16 MAC provides QoS differentiation for the different types of applications that might operate over 802.16 networks, through five defined scheduling service types, also called QoS classes. To perform QoS implies that various negotiated performance indicators that are tied to the overall QoS must be met for each connection (e.g. latency, jitter, data rate, packet error rate, system availability, etc.) [JGA06].

Scheduling Services The IEEE MAC uses a scheduling service to deliver and handle SDUs and MPDUs through the respective service flow (with QoS requirements associated). A scheduling service uniquely determines the mechanism the network uses to allocate uplink and downlink transmission opportunities for the PDUs. Each scheduling service, or service classes, have associated QoS parameters. There is defined five scheduling services [JGA06]:

1. **Unsolicited Grant Service (UGS)** - is designed to support real-time service flows consisting of fixed-size data packets issued at periodic intervals. This would be the case, for example, Voice over Internet Protocol (VoIP) without silence suppression. UGS offers fixed-size grants on a real-time periodic basis and does not need the SS to explicitly request bandwidth, thus eliminating the overhead and latency associated with bandwidth request.

2. **real-time Polling Service (rtPS)** - is designed to support real-time services that generate variable-size data packets on a periodic basis, like video streaming. In this service class, the BS provides unicast polling opportunities for the SS to request bandwidth. This service requires more request overhead than UGS does but is more efficient for service that generates variable-size data packets.

3. **nonreal-time Polling Service (nrtPS)** - is very similar to rtPS except that the SS can also use contention-based polling in the uplink to request bandwidth. In nrtPS, it is allowable to have unicast polling opportunities, but less often are more spaced than the rtPS. It is also possible to request resources during the contention-based polling opportunity, which can often result in collisions and additional attempts.

4. **Best Effort (BE)** - provides very little QoS support and is applicable only for services that do not have strict QoS requirements. Data is sent whenever resources are available and not required by any other scheduling-service classes.

[3]The scheduling algorithm has a profound impact on the overall capacity and performance of the system, it can be a key feature distinguishing among implementations of various equipment manufacturers.

5. **extended real-time Polling Service (ertPS)** - (used only in Mobile WiMAX) is a new scheduling builds on the efficiencies of UGS and rtPS. In this case, periodic uplink allocations provided for a particular SS can be used either for data transmission or for requesting additional bandwidth. Is used for applications like VoIP with silence suppression.

Service Flow A service flow is a MAC transport service provided for transmission of uplink and downlink traffic and is a key concept of the QoS architecture [JGA06]. Each service flow is associated with a unique set of QoS parameters, such as latency, jitter throughput, and packet error rate, that the system strives to offer. A service flow is constituted by [JGA06]:

- **SFID** - a 32-bit identifier for the service flow.
- **CID** - a 16-bit identifier of the logical connection to be used for carrying the service flow.
- **Provisioned QoS parameter set** - the recommended QoS parameters to be used for the service flow, usually provided by a higher-layer entity.
- **Admitted QoS parameter set** - the QoS parameters actually allocated for the service flow and for which the BS and the MS reserve their PHY and MAC resources.
- **Active QoS parameter set** - the QoS parameters being provided for the service flow at any given time.
- **Authorization module** - logical BS function that approves or denies every change to QoS parameters and classifiers associated with a service flow.

Bandwidth Request/grant mechanism

The bandwidth request/grant mechanism for the IEEE 802.16 standard was chosen to be efficient, low-latency, and flexible and to dovetail with QoS [CE06]. Requests are made from the SSs to the BS on a connection basis (CID basis) to ensure they can be properly used fair algorithms in the BS's UL scheduler. But grants (bandwidth attributions) are made to the SS, not to the connection. This increases efficiency and reduces the latency can also be reduced. Is important to refer that in the downlink, the BS schedules MPDUs for the PHY resources, based on their QoS requirements, and indicated that to the SS using the DL-MAP massage. For the uplink, there is no explicit acknowledge message for requests. Either the SS gets a grant, or it does not (this saves the bandwidth that would have been used for the acknowledgments).

In the uplink, the SS requests resources by either using a stand-alone bandwidth-request MPDU or piggybacking bandwidth requests on a generic MPDU (grant-management sub-header). All resource requests are made in terms of bytes of information, rather than PHY resources, such as number of subchannels and/or number of OFDM symbols, because the burst profile associated with a CID can change dynamically [JGA06]. Bandwidth requests in

the UL can be incremental or aggregate requests. The bandwidth requested by piggybacking on a MPDU can be only incremental.

Polling refers to the process whereby dedicated or shared UL resources are provided to the SS to make bandwidth requests [IEE04]. These allocations can be for an individual SS (unicast) or a group of SSs (multicast/broadcast). SSs that have an active UGS connection are not polled, since the bandwidth request can be sent on the UGS allocation either in the form of a bandwidth request PDU or by piggybacking on generic MPDUs. A dummy packet must be send during the unicast polling if the SS don´t have additional bandwidth requirements (silent during the unicast polling is not allowed).

If there is now sufficient bandwidth to poll each SS individually, multicast or broadcast polling is used to poll a group of users or all the users at a time. All SSs belonging to the polled group can request bandwidth during the multicast/broadcast polling opportunity. It is allocated in the uplink subframe a bandwidth requests contention slot that allows multiple SSs to compete for a transmission opportunity to send the bandwidth request. The IEEE 802.16 defines a contention resolution algorithm for SSs get the transition opportunity (in case of collisions).

3.5.3 Security Sublayer

The IEEE 802.16 security sublayer consists of two components: an encapsulation protocol for encrypting MAC payloads and a key management protocol called Privacy Key Management (PKM). The encapsulation defines the encryption and data authentication method and the rules specifying how to apply these to the MPDU payload. The MAC headers are sent unencrypted. The subheaders, however, are encrypted as they are considered part of the payload. The majority of the MAC management messages are not encrypted, but integrity protection is afforded to management messages to prevent theft of service.

The encapsulation protocols are [CE06]:

- Data Encryptio Standard (DES) in cipher block chaining (CBC) mode - which only encrypts the data but offers no integrity protection. The CBC initialization vector is derived from the frame number, and thus there is no data expansion as a result of applying this protocol. Due to use of the DES algorithm and the way it is used, this encapsulation does not offer a high level of security;

- Advanced Encryption Standard (AES) with counter with CBC-MAC - which is much better security in encapsulating MPDU payloads. In addition to strong encryption, it also affords data integrity protection. The inconvenience of this protocol is that the size each MPDU is increased by 12 bytes.

The IEEE 802.16 key management protocol supports secure distribution of keys from BS to SS. The BS may use the key management protocol to enforce conditional access to network services. The SS use this PKM protocol to authorize traffic and obtain keys from the BS and performs periodic reauthorization and key refresh. Per BS, a unique X.509 digital certificates and RSA public-key encryption algorithms are used to perform key exchanges between SS

and BS. The IEEE 802.16 MAC provides MAC management support for transporting PKM messages between BS and SS. The PKM protocol uses public-key cryptography to establish a shared secret between SS and BS, and the shared secret is used to secure subsequent PKM exchanges.

The IEEE 802.16e-2005 [IEE05b] introduces support for Extensible Authentication Protocol (EAP) and a new version of the key management protocol (PKM version 2) that takes into consideration the issues brought into play a mobile network [CE06].

3.6 IEEE 802.16 PHY

The IEEE 802.16 standards defines within its scope five PHY layers, any of which can be used with the MAC to develop a broadband wireless system. The PHY layers defined in IEEE 802.16 are [IEE04] [IEE05b]:

- WirelessMAN single carrier (SC) - a single-carrier PHY layer intended for frequencies from 11 to 66GHz requiring a LOS condition. This PHY layer is part of the original 802.16 specifications.
- WirelessMAN SCa - a single-carrier PHY for frequencies between 2GHz and 11GHz for PMP operations.
- WirelessMAN OFDM - a 256-point FFT-based OFDM PHY layer for PMP operations in NLOS conditions at frequencies between 2GHz and 11GHz. This PHY layer, finalized in the IEEE 802.16-2004 specifications, has been accepted for Fixed WiMAX.
- WirelessMAN OFDMA - a 2,048-point FFT-based OFDMA PHY for PMP operations in NLOS conditions at frequencies between 2GHz and 11GHz, as defined in IEEE 802.16-2004 [IEE04]. In the IEEE 802.16e-2005 [IEE05b] standard, this PHY layer has been modified to Scable Orthogonal Frequency Division Multiple Access (SOFDMA), where the FFT size is variable and can take any one of the following values: 128, 512, 1,024, and 2,048. this size allows for optimum operation/implementation of the system over a wide range of channel bandwidths and radio conditions. This PHY layer has adopted for Mobile WiMAX.
- WirelessHUMAN - in IEEE 802.16-2004 [IEE04] is also define a PHY scheme for unlicensed frequency bands (High-speed Unlicensed Metropolitan Area Network (HUMAN)).

Like was mention before, the WiMAX physical layer is based on OFDM. OFDM has adopted because this is an elegant and efficient scheme for high data rate transmission in a NLOS or multipath radio environment [JGA06].

The IEEE 802.16 WirelessMAN OFDM and WirelessMAN OFDMA PHY is responsible to receive the MAC PDUs and send it over the air. At this layer, can be distinguish two main functions: build the PHY frame (slot and frame structure); and transmit/receive data into/from air.

3.6.1 Slot and Frame Structure

In IEEE 802.16, both, FDD and TDD, duplexing schemes are allowed. In the case of FDD, the UL and DL subframes are transmitted simultaneously on different carrier frequencies. In the case of TDD, the UL and DL subframes are transmitted on the same carrier frequency at different times. The frame structure for the FDD mode is identical except that the UL and DL subframes are multiplexed on different carrier frequencies.

The minimum time-frequency resource that can be allocated by a WiMAX system to a given link is called a slot. Since OFDM and OFDMA frames are different, those have to be described in separated.

OFDM Frame

In figure 3.9 is represented the OFDM frame structure in TDD mode. An OFDM PHY DL subframe consists of only one DL PHY PDU, which can be shared by more than one SS. A DL PHY PDU starts with a long preamble, which allows PHY synchronization for listening SSs [Nua07]. A listening SS synchronizes to the DL using the preamble. The preamble is followed by a frame control header (FCH) burst. The FCH contains the downlink frame prefix (DLFP) which specifies the burst profile and length of at least one DL burst immediately following the FCH. The standard indicates that the DLFP is one OFDM symbol with the most robust modulation and coding scheme (modulation BPSK and coding 1/2). A DL-MAP message, which indicates of the downlink frame use, if transmitted in the current frame, must be the first MAC PDU in the burst following the FCH. A UL-MAP message, which indicator of the uplink frame use, immediately follows either the DL-MAP message (if there is one) or the FCH. If uplink channel descriptor (UCD) and UCD messages are transmitted in the frame, they immediately follow the DL-MAP and UL-MAP messages. These downlink bursts are transmitted in order of decreasing robustness of their burst profiles (indicated by downlink interval usage code (DIUC) and uplink interval usage code (UIUC)).

The OFDM PHY UL subframe is constituted by three main parts [Nua07]:

- Contention slots for initial ranging. This is a BS specified interval in which new stations may join the network. Packets transmitted in this interval use specific MAC management message (RNG-REQ) and are transmitted using a contention procedure as collision(s) may occur with other incoming SSs.
- Contention slots for bandwidth requests.This is a BS specified interval in which requests may be made for a bandwidth for uplink data transmission.
- One or many uplink SS PDUs, each transmitted on a burst. Each of these PDUs is an UL subframe transmitted from a different SS.

OFDMA Frame

For the OFDMA PHY, the frame format is evidently different, taking into account that data mapping is made on two dimensions: time and subcarriers (figure 3.10). As in the OFDM

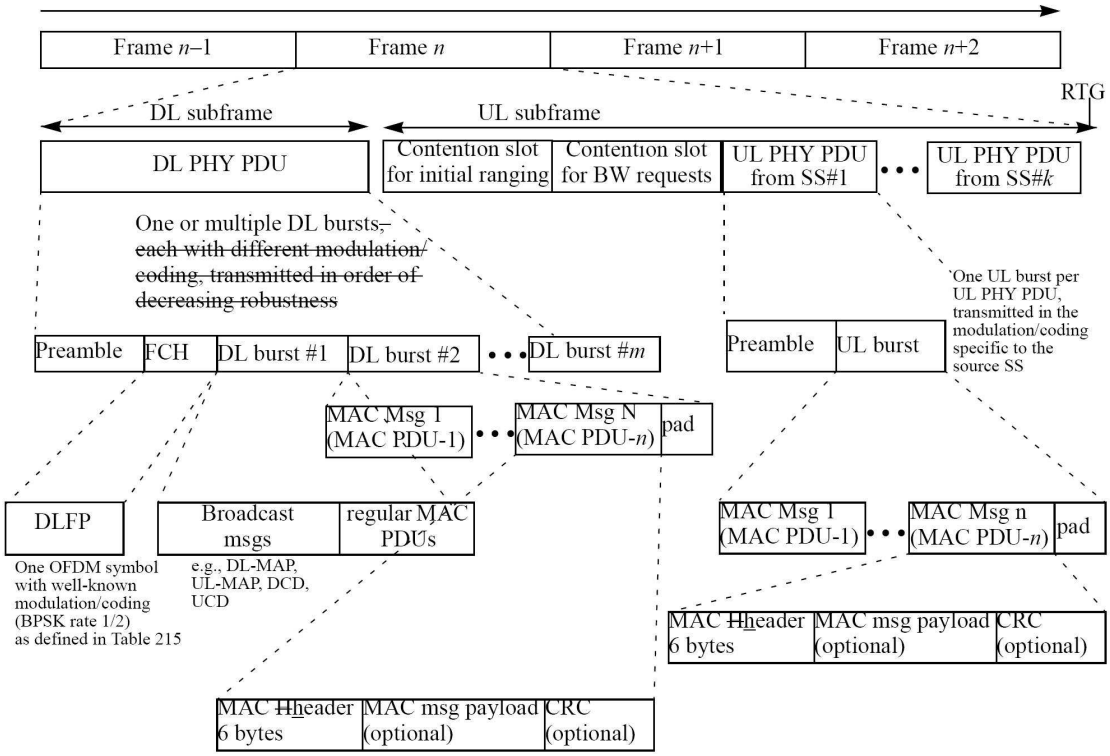

Figure 3.9: OFDM Frame in TDD mode, from [IEE05b]

PHY, frist there is a DL preamble and then the FCH, which has a fixed location and duration in the frame and contains only the DLFP [CE06]. The DLFP specifies the subchannel groups of which the segment is constructed, the length of the DL-MAP, how much repetition coding is used on the DL MAP, and whether there is any change to the ranging allocation from the previous frame.

The MAPs in specify the permutation zones[4], where the first is mandatory (Partial Usage of Subchannels (PUSC)). The MAPs also specify the location and content of all bursts.

The framing structure used for the uplink includes an allocation for ranging and an allocation for data transmission. The MAC layer sets the length of the uplink framing and the uplink mapping [IEE05b].

3.6.2 Transmitting over the air

In figure 3.11 is represented the functional stages of the PHY in transmission mode. The first set of functional stages is related to channel coding (randomization, FEC, interleaving, repetion and modulation). Then, the next set of functional stages is related to the construction of the PHY symbol in the frequency domain. In this stage, data is mapped onto

[4]Permutation zone is a set of OFDM symbols which the same mapping of logic subchannels to physical subcarriers is used.

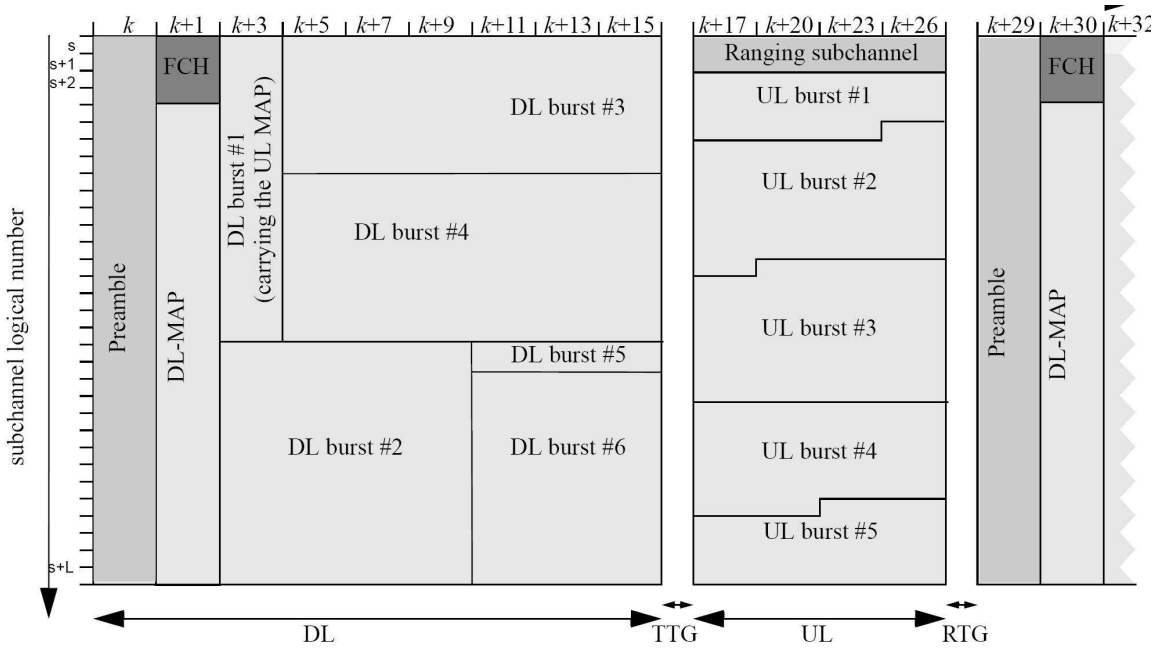

Figure 3.10: OFDMA Frame in TDD mode, from [IEE05b]

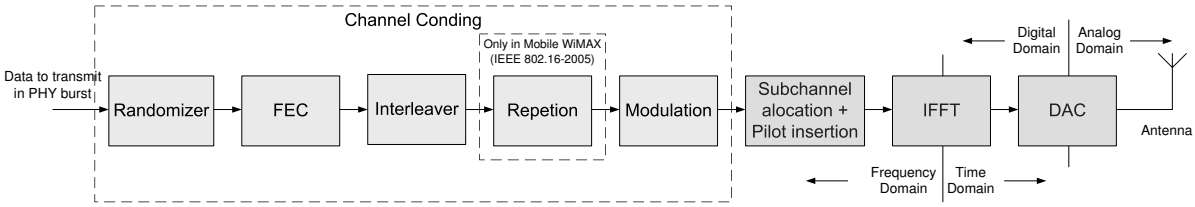

Figure 3.11: Stages of WiMAX PHY transmission, adapted from [JGA06] [IEE05b]

---

the appropriate subchannels and subcarriers. Also pilot symbols are inserted into the pilot subcarriers, which allows the receiver to analyze the channel information. The final set of functions is related to the conversion of the OFDM symbol from the frequency domain to the time domain and to an analog signal that can be transmitted over the air.

Channel coding

Randomization As is cited in [CE06]: "*a specific sequence of data modulated on an OFDM symbol results in a given peak to average power ratio (PAPR) for that symbol. With a small probability of occurrence, this PAPR can quite large (e.g., more than 7dB). It is generally inefficient to back the transmitter power amplifier off far enough to avoid unrecouverable non-linear distortion at the worst possible PAPR. Practical designs instead back off the amplifier*

only far enough to keep the probability of unrecouverable distortion acceptably low. However, retransmitting a data sequence with a high PAPR would result in a repeated received error". So, the randomizer block can avoid such persistent errors.

FEC This block can detect and correct some errors upon the reception by adding redundancy to the transmitted signals [CE06]. For OFDM PHY are specified three methods of channel coding: Reed-Solomon concatenated with convolutional coding (RS-CC) (mandatory), block turbo code (BTC) (optional), and convolutional turbo code (CTC) (optinal) [IEE04]. For OFDMA PHY are specified five methods of channel coding: convolutional coding (CC) with tail-biting, BTC, and CTC, low-density parity check coding (LDPCC), and CC with zero-tailing. Only the first one is mandatory [IEE05b].

Interleaver Interleaving is used to protect the transmission against long sequences of consecutive errors, which are very difficult to correct. The OFDMA PHY uses a different interleaver than that is used by OFDM PHY [CE06], which is divide in two parts:

- Distribute the coded bits over subcarriers. A first permutation ensures that adjacent coded bits are mapped on to nonadjacent subcarriers;
- The second permutation insures that adjacent coded bits are mapped alternately on to less or more significant bits of the constellation, thus avoiding long runs of bits of low reliability.

Repetion Repetition was added by the IEEE 802.16-2005 [IEE05b] for OFDMA PHY. The standard indicates that it can be used to increase the signal margin further over the modulation and FEC mechanisms.

Modulation For OFDM PHY and OFDMA PHY is mandatory to support BPSK as well as Gray-mapped 4-QAM (QPSK) and 16-QAM constellations. The Gray-mapped 64-QAM constellation is optional. The pilots subcarries are modulated with a BPSK signal [CE06].

OFDM Symbol Structure

OFDM is a multiplexing technique that subdivides the bandwidth into multiple frequency sub-carriers [Pap08a]. First, the OFDM signal is constructed in the frequency domain and then, using the inverse fast Fourier transform (IFFT), is converted to time domain. In the frequency domain, each OFDM symbol is created by mapping the sequence of symbols on the subcarriers. In IEEE 802.16 standard [IEE04] has three classes of subcarriers:

1. **Data subcarriers** are used for carrying data symbols;
2. **Pilot subcarriers** are used for carrying pilot symbols. The pilot symbols are known a priori and can be used for channel estimation and channel tracking.

3. **Null subcarriers**, including the DC subcarrier and the guard subcarriers. The DC subcarrier is not modulated, to prevent any saturation effects or excess power draw at the amplifier. No power is allocated to the guard subcarrier toward the edge of the spectrum in order to fit the spectrum, of the OFDM symbol within the allocated bandwidth and thus reduce the interference between adjacent channels.

The IFFT creates the useful OFDM symbol time. As demand of OFDM theory [Nua07], the cyclic prefix (CP) must be add at the be added at the beginning of the symbol. The CP is a repetition of the last samples of useful data portion of the symbol, which can prevents the inter-block interference and eliminate the intersymbol interference (ISI) as long as the CP duration is longer than the channel delay spread.

3.7 Summarized comparison between Fixed and Mobile WiMAX

As mention above, the WiMAX Forum defines two versions of WiMAX:

- **Fixed WiMAX** - this is based on the IEEE 802.16-2004. It uses OFDM and supports fixed and nomadic access in LOS and NLOS environments.
- **Mobile WiMAX** - Optimized for dynamic mobile radio channels, this version is based on the is based on the IEEE 802.16-2005 and provides support for handoffs and roaming. It uses SOFDMA, a multi-carrier modulation technique that uses sub-channelization.

The figure 3.12 presents a comparision between the IEEE 802.16 standards, in order to resume the basic characteristics of WiMAX as radio communication technology.

	802.16	802.16-2004	802.16e-2005
Status	Completed December 2001	Completed June 2004	Completed December 2005
Frequency band	10GHz–66GHz	2GHz–11GHz	2GHz–11GHz for fixed; 2GHz–6GHz for mobile applications
Application	Fixed LOS	Fixed NLOS	Fixed and mobile NLOS
MAC architecture	Point-to-multipoint, mesh	Point-to-multipoint, mesh	Point-to-multipoint, mesh
Transmission scheme	Single carrier only	Single carrier, 256 OFDM or 2,048 OFDM	Single carrier, 256 OFDM or scalable OFDM with 128, 512, 1,024, or 2,048 subcarriers
Modulation	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM	QPSK, 16 QAM, 64 QAM
Gross data rate	32Mbps–134.4Mbps	1Mbps–75Mbps	1Mbps–75Mbps
Multiplexing	Burst TDM/TDMA	Burst TDM/TDMA/ OFDMA	Burst TDM/TDMA/ OFDMA
Duplexing	TDD and FDD	TDD and FDD	TDD and FDD
Channel bandwidths	20MHz, 25MHz, 28MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz	1.75MHz, 3.5MHz, 7MHz, 14MHz, 1.25MHz, 5MHz, 10MHz, 15MHz, 8.75MHz
Air-interface designation	WirelessMAN-SC	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[a]	WirelessMAN-SCa WirelessMAN-OFDM WirelessMAN-OFDMA WirelessHUMAN[a]
WiMAX implementation	None	256 - OFDM as Fixed WiMAX	Scalable OFDMA as Mobile WiMAX

a. WirelessHUMAN (wireless high-speed unlicensed MAN) is similar to OFDM-PHY (physical layer) but mandates dynamic frequency selection for license-exempt bands.

Figure 3.12: Basic characteristics on IEEE 802.16 Standards, from [JGA06]

Chapter 4

Evaluation of WiMAX Network entry procedures for vehicular communication

4.1 Introduction

The evaluation of an equipment for road safety vehicular communications requires a deep analysis of the several parts of the system, from the radio frequency (RF) element features to the end applications used for road safety management. As mentioned before, WiMAX has not been projected for road safety vehicular communications, so, considering the use of WiMAX as transportation technology in this context, it is important to verify if real-time requirements for this type of application are achieved.

One important process that has to be evaluated when using WiMAX for road safety applications is the network entry. Network entry is the process that a SS (or MS) needs to perform in order to get connected to a BS. The IEEE 802.16 standards (which defines the WiMAX MAC and PHY) defines the steps that a SS has to do to access the network (connect to a BS). To analyze these steps and to match them to the needs of vehicular communication scenarios is the main objective of this chapter. The network entry process defined in IEEE 802.16 standards refers to the MAC level, and presents some differences depending on the PHY that is in use (OFDM for Fixed WiMAX; or OFDMA for Mobile WiMAX).

4.2 Timing analysis of IEEE 802.16 Network Entry

4.2.1 Overview

Once the SS is powered up, it begins the boot and initialization process. In a PMP topology, this process consists in the following steps [CE06]:

1. *Search and synchronize with the BS (scanning)* - the first step that the SS has to do, before anything else, is to find a valid BS signal. For that, the SS chooses a predefined

frequency channel and starts searching the downlink frame preamble.

2. *Acquired transmission parameters* - once the SS finds the preamble, it tries to determine the downlink and uplink transmissions parameters.

3. *Initial Ranging* - this process has the finality of adjusting the transmission power for optimal BS reception, allocating the SS basic and primary management CIDs; and, for FDD and half-duplex frequency division duplexing (H-FDD) systems, adjusting the uplink frequency.

4. *Basic capability negotiation* - once all the parameters from the initial ranging process have been adjusted, the SS needs to tell the BS which optional functionalities it supports and, conversely, the BS needs also to inform the SS about which optional features it can use. The optional features covered by the process are only those having to do with MAC and PHY.

5. *Authorization, security association (SA) establishment and key exchange* - at this stage, the BS does not know completely the identity of the SS. The SS has already provided its MAC address but has offered no credentials to allow the verification of its identity. The authorization phase establishes the SS identity, the authorization key and the list of SAs that the SS can use.

6. *Perform Registration* - During this process the SS and BS negotiate some additional MAC parameters and the SS informs the BS if it will be part of the managed network (managed SS). If so, the secondary management connection (bidirectional) is established between BS and SS. The registration message also allows negotiating the IP version and QoS parameters for the secondary management connection.

7. *Establishing IP connectivity* - If the SS is managed and a secondary management was set then it needs to acquire a dynamic IP address (using DHCP), download a configuration file using TFTP and establish the time of the day using Internet Time Protocol, being these two last steps optional.

8. *Establishing connection* - Before starting data communication it is necessary to establish a dynamic service. For a managed SS this begins when the reception of the TFTP configuration file is concluded and for an unmanaged SS it begins when the registration process is concluded.

4.2.2 Search and synchronize with the BS (scanning)

Before the SS can do anything else, it has to find first a BS transmitting a signal that it is capable of decoding and understanding. To perform this, the SS consults a frequency lists, chooses one of the channels mentioned in the list, and starts to search for the periodically occurring frame preamble. The IEEE 802.16-2004 [IEE04] defines that the SS must have a nonvolatile memory to store the last operational parameters. The SS must use the last operational parameters for the first synchronization trial. If that fails, it shall begin to

continuously scan the possible channels of the downlink frequency band of operation until it finds a valid downlink signal. In IEEE 802.16e-2005 [IEE05b], SS tries to reacquire the last downlink parameters is optional, as so the continuously scanning in the downlink frequency band (jump between channels are allowed). In both standards, is defined that **a search in a single channel should be at least at least 2 MAC frames** duration, before going forward to the next channel. The IEEE 802.16 standards defines a maximum frame duration of 20 ms[1].

4.2.3 Acquired transmission parameters

Obtain downlink parameters

When the SS finds the preamble, it tries to determine the DL transmission parameters by looking at the FCH and the DL-MAP and downlink channel descriptor (DCD) messages. The MAC synchronization is achieve once the SS received one DL-MAP message. The **maximum time** that a SS is allowed to **search for DL-MAP message in the same channel** is **10 s** by [IEE04] or **11 s** by [IEE05b]. If that time is achieve without finding the DL-MAP message, the synchronization process should restart. When a DL-MAP is found, it should be wait for a DCD message. As defined in the IEEE 802.16, the periodicity of this message should be at most of 10 s. If five times of that, equal to **50 s**, have passed **without a DCD message received** SS should restart synchronization.

After received the first DL-MAP message, it should also restart if **600 ms** have passed without receiving another DL-MAP message.

Obtain uplink parameters

After the downlink synchronization, the SS shall wait for a UCD message from the BS in order to retrieve a set of transmission parameters for the uplink channel. Like the DCD message, the UCD message should be transmitted periodically with the maximum interval of 10 s [IEE04]. The synchronization process in the SS should restart if five times of that time (**50 s**) have passed **without received a UCD message**. After received the first UCD message, it should start the reception of the **UL-MAP message**, which is also periodic, and must appears in a **interval of 600 ms**. If not, the synchronization should restart.

4.2.4 Initial Ranging

The initial ranging first objective is to obtain the relative timing and power-level adjustment required to maintain the uplink connection with the BS [JGA06]. Then, is allocated the Basic and Primary management CIDs. Once the a uplink connection has been established, the SS should do periodic ranging to track timing and power-level fluctuations.

The SS shall scan the UL-MAP message to find an Initial Ranging Interval. This interval defines the time between Initial Ranging regions assigned by BS, which can get the maximum of 2 s. The SS should restart downlink synchronization if fives times of that interval

[1]For both PHY, OFDM and OFDMA, the frame duration can be: 2, 2.5, 4, 5, 8, 10, 12.5 and 20 ms [IEE04]

(**maximum of 10 s**) has occurred **without a Initial Ranging region**. Since the SS does not have a connection established at this point, the initial ranging opportunity is contention based. At this stage, the process is different depending of PHY that is in used.

For OFDM PHY, the SS send a RNG-REQ message with the CID set to *initial ranging CID* (equal to zero), with a transmission power previous calculate based on DCD message information and from the received signal strength indicator (RSSI). The SS should **wait a response** (RNG-RSP message) for the **maximum of 200 ms** after sending the RNG-REQ message. This time is also applicable for others RNG-REQ messages that are send. If SS doesn´t receive any RNG-RSP message in that time, it should retry until the **number of ranging request retries**, **at least 16**, be achieved. If that happens, the SS should start for another downlink channel. Once the BS has successfully received the RNG-REQ message, it shall return a RNG-RSP message using the initial ranging CID. Within the RNG-RSP message shall be the Basic and Primary Management CIDs assigned to this SS. At this point the BS shall start using invited Initial Ranging Intervals addressed to the SS´s Basic CID to complete the ranging process, unless the status of the RNG-RSP message is success, in which case the initial ranging procedure shall end. If the status of the RNG-RSP message is continue, the SS shall wait for an individual Initial Ranging interval assigned to its Basic CID. Using this interval, the SS shall transmit another RNG-REQ message using the Basic CID along with any power level and timing offset corrections. This process shall be repeat until the response contains a ranging successful notification or the BS aborts ranging. If BS aborts ranging, SS should start scan for a different downlink channel.

For the OFDMA PHY, SS should send code division multiple access (CDMA) ranging code. For that, choose randomly a Ranging Slot then it chooses randomly a Ranging Code and sends it to the BS (CDMA mechanism). The transmission power is also calculate from the DCD message information and also from the RSSI. Similiar to OFDM PHY, the SS should **wait a response** for the **maximum of 200 ms**, if not, it should retry for **at least 16** times. When the BS receive the CDMA ranging code, it cannot tell which SS sent the CDMA ranging request. So,the BS broadcasts a Ranging Response message (RNG-RSP) that advertises the received Ranging Code as well as the ranging slot where the CDMA Ranging code has been identified. This information is used by the SS that sent the CDMA ranging code to identify the Ranging Response message. The RNG-RSP message contains all the necessary adjustment information (e.g. power level) and a status notification. Upon receiving a Ranging Response message with continue status, the SS shall continue the ranging process as done on the first entry with ranging codes randomly chosen from the Initial Ranging domain sent on the Periodic Ranging region. When the BS receives an initial-ranging CDMA code that results in sending an RNG-RSP message with success status, the BS shall provide bandwidth allocation for the SS to send an RNG-REQ message. Initial ranging process is over after receiving RNG-RSP message including a valid basic CID. If this RNG-RSP message includes "continue" indication, the ranging process should be continued using the periodic ranging mechanisms.

4.2.5 Basic capability negotiation

After the initial ranging, the SS informs the BS of its basic capabilities by transmitting an SBC-REQ message with basic capability set, which includes various PHY parameters, like the support of 64-QAM modulation, the Authorization Policy support, and others [IEE05b]. After the BS send the RNG-RSP message with the status of "success" (at the of of initial ranging), it should wait for a SBC-REQ for at the minimum of 300 ms. In other way, the SS, after sending the SBC-REQ message, it should **wait for a BS response** (SBC-RSP) for the **maximum of 50 ms**. Then it should **retry send the SBC-REQ at least 3 times** and **at most of 16 times**. If no SBC-RSP have been received, the SS should restart the network entry process. Note that the basic capabilities approved by the BS can be the set of the SS basic capabilities or a subset of it.

4.2.6 Authorization, SA establishment and key exchange

If the authorization policy is supported, the BS and BS shall perform authorization and key exchange. For IEEE 802.16-2004 [IEE04], the authorization policy is mandatory to support, and not included in the basic capabilities negotiation. For IEEE 802.16e-2005 [IEE05b], this step is optional and negotiated at this stage.

The authorization protocol starts with the SS sending the authentication information PKM message. All PKM messages are encapsulated in either the PKM-REQ (SS to BS) or the PKM-RSP (BS to SS) management message [CE06]. First, SS send Authentication Information to the BS, which is only informational (contains the X.509 certificate). Then, the SS send the Authorization Request message which includes its security capabilities. If authorization is well succeed, the BS send the Authorization Reply message contain a authorization key (AK) and a list of SAs. After this, SS becomes authorized[2]. The IEEE 802.16 standards defines that each SS have **at least 5 minutes to perform all authorization process**.

4.2.7 Perform Registration

During the registration phase, the SS and BS negotiated additional operational parameters of the MAC. Also, the SS informs the BS whether it will be part of the managed network (managed SS). If the SS is to be managed, the bidirectional secondary management connection is established between the SS and BS. The registration message exchange also offers the possibility to negotiate the version of IP and the CID of the secondary management connection. For execute the registration process, SS sends a REG-REQ message and **wait for a REG-RSP** message from the BS **at most of 3 s**. If there isn´t no REG-RSP received or if the REG-RSP don´t have the status "OK", it should **retransmit the REG-REQ message at least for 16 times**.

After the registration process, if the SS is not a managed SS, it should establish provisioned connections. If that is a managed SS, it should try to establish IP connectivity.

[2]At this stage, SS is only allowed to transmit MAC management messages. For become full operational, the SS needs to acquire a key for each SA (traffic encryption key (TEK))

4.2.8 Establishing IP connectivity

A managed SS also needs to acquire an IP addressing (using DHCP), pull down a configuration file (using TFTP), and establish the time of day (using the Internet Time Protocol) [CE06]. Getting a configuration file and establish time of day is not mandatory for a managed SS [IEE04]. In order to obtain an IP address (and other parameters) to establish IP connectivity, the SS shall invoke DHCP mechanisms defined in Internet Engineering Task Force (IETF) RFC 2131 [IET97]. No time restriction is indicated at the IEEE 802.16 for get IP connectivity (DHCP dependent). For establish the time of day, the SS should follow the mechanisms described by IETF RFC 868 [IET83]. For this, **no more than 3 requests** should be done in a **window of 5 minutes**. For get the configuration file, the SS should use the TFTP protocol to transfer that. After successfully received the the configuration file, it should send a TFT-CPLT message to confirm the reception of the file. Then, the BS an acknowledge message (TFT-RSP). In the IEEE 802.16 standards is define that BS shall **wait at least 15 minutes** since the **transmission of a registration response** (REG-RSP) **to the receive of the TFT-CLPT**. If SS don´t receive a successful TFT-RSP message, it should **retry at least for 16 times**.

4.2.9 Establishing provisioned connections

The final step before actual data communication begin in a dynamic service establishment. In the case of a management SS entering the network, the reception of the TFTP-CPLT (configuration file TFTP complete) message triggers the BS to start connection setup. When dealing with unmanaged SSs, the successful completion of registration process serve as the trigger. The service flows for a given SS are assumed to have been provisioned by the BS. To activate them or take them to the admitted, the BS initiates a dynamic service addition (DSA) exchange (figure 4.1). For that, it sends the DSA-REQ message and shall **wait for a SS response** (DSA-RSP) indicating acceptance or rejection in a period of time **lower than 1 s**. Finally, the BS sends an acknowledged message (DSA-ACK) in a period of time **lower than 300 ms**. After at least one service flow has been activated, the SS is capable of sending or receiving user data.

4.2.10 Summary of Network Entry Steps

In figure 4.2 a summary of the time considerations that the IEEE 802.16 standards defines is represented. One of the main considerations that is defined is the timeout to wait for a message: after a request (RNG-RSP wait timeout) or simple search for a message (DL-MAP wait timeout). It is also defined the number of retries that have to be done for some messages.

In the acquisition of transmission parameters, all four MAC messages (DL-MAP, UL-MAP, DCD and UCD) can be taken into a single frame, and so reducing the acquisition time to a single frame. It must be considered, in a exchange of request/response messages, that it is necessary to have a frame for the request and another for the response, this in a TDD system[3]. Like is mention above, The Initial Ranging process is different depending on the

[3]If the request is send in the downlink, there is nothing that not allow the SS to send the response on the

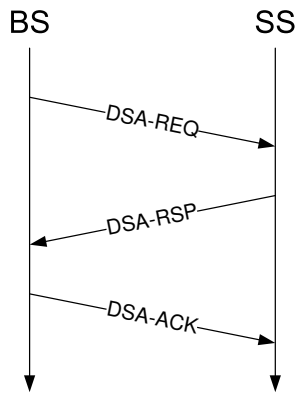

Figure 4.1: DSA message flow (BS initiation), adapted from [IEE04]

PHY that is in used. Although looks like the OFDMA Initial Ranging process is longer than the OFDM (if no retries needed), this can be faster in a collision scenario, where multi-users try to connect to the BS [CE06].

4.2.11 Network Entry example

In the study above, it is presented the IEEE 802.16 Network Entry process (relevance for messages flows) and the time restrictions that are associated. However, it isn't defined any specific time to execute the whole process. To determine the network entry time it is needed to take into consideration some aspects like the WiMAX version that is in use or the frame duration in use. The analysis of the worst case for network entry can lead to unrealistic and not acceptable times, even for a fixed system. For example, waiting for a DCD message in the *acquisition transmission parameters* step can take up to 50 s (the same time is necessary to wait the UCD message in worst case). And this is just a single step in the network entry process.

In order to determine the Network entry execution time, next some issues will be discussed. First, it is necessary to choose which version of WiMAX is intended to be used (Fixed or Mobile), which implies a different Initial Ranging process[4] and optional performs the Authorization process in the case of Mobile WiMAX. Then, it is necessary to choose if the SS is managed or not managed. If the SS is managed, that implies the execution of the *Establish IP connectivity* step to acquire the IP address (using DHCP) and, optionally, to get the time and date (using Time Protocol) and to transfer the configuration file (using TFTP). Since a managed SS implies the execution of several WiMAX external protocols, it will not be taken into consideration in this example. Another important choice to be made is the topology. In a FDD topology, the exchange of messages can be faster than in the TDD or in the H-FDD topologies, because the uplink subframe can occur simultaneously with the downlink

uplink part of the same frame (TDD system also)

[4] OFDM PHY for Fixed WiMAX; OFDMA PHY for Mobile WiMAX

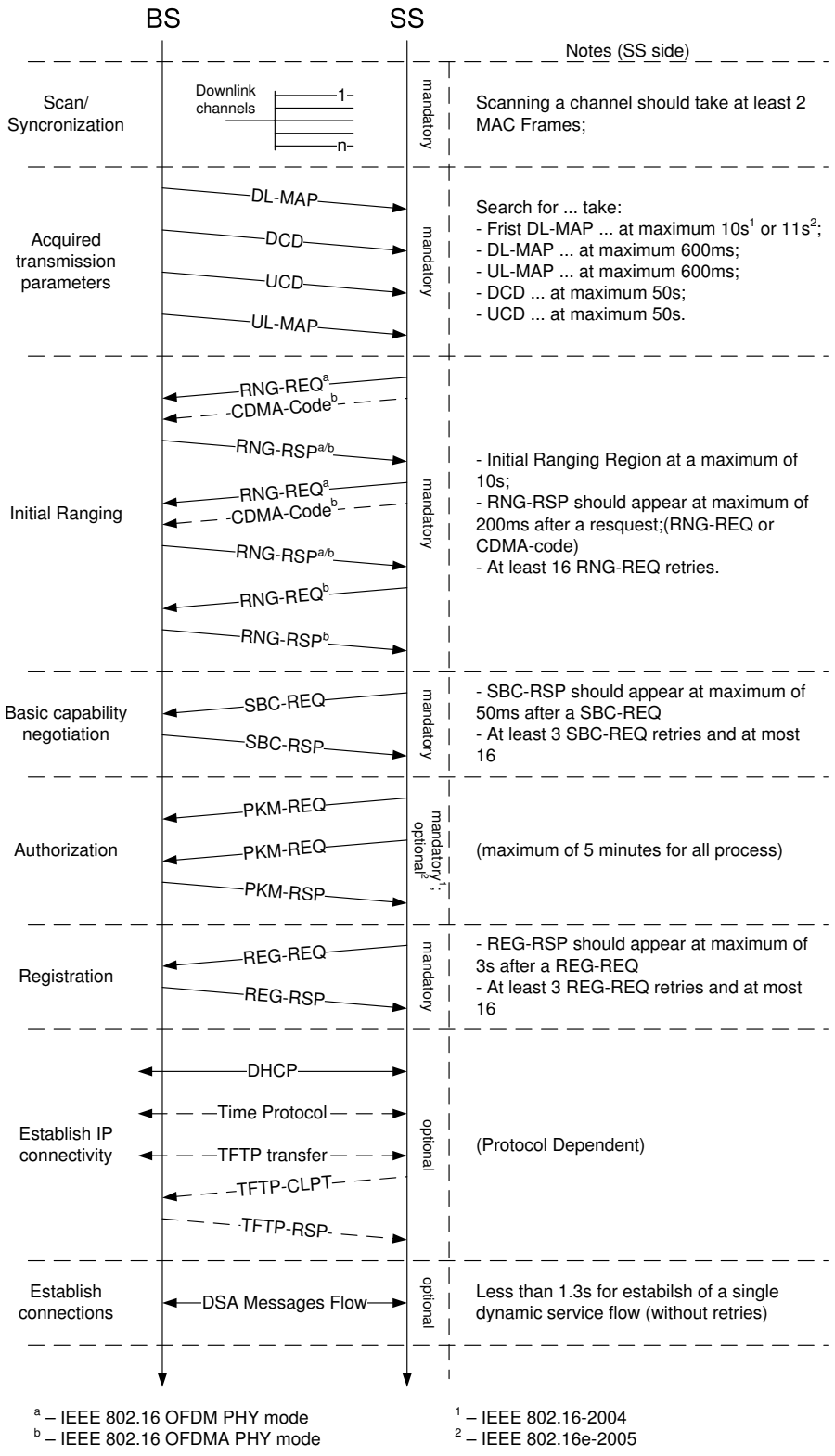

Figure 4.2: IEEE 802.16 Network Entry message flow

Parameters	Value	Description
WiMAX Version	Fixed	
Managed SS	no	
Topology	TDD	
Frame Duration	10 ms	
Number of channels	3	
Scan in each channel	100 ms	10 frames
Synchronization to DL-MAP	60 ms	6 frames
DL-MAP to DCD	20 ms	2 frames
DCD to UCD	20 ms	2 frames
UCD to UL-MAP	20 ms	2 frames
UL-MAP to Initial Ranging	40 ms	4 frames
Message REQ to Message RSP and Message RSP to Message REQ	10 ms	1 frame
Time between steps	20 ms	2 frames
Messages retransmissions	No	

Table 4.1: Network Entry example parameters

subframe. For a simple analysis, it would be considered a TDD system, and the time between a request message and a response message should be at least one frame duration, although that time can be shorter.

Example Time Calculation

Table 4.1 shows the parameters that were chosen to calculate an example of the time required for Network Entry. The number of channels equal to 3 means that a SS can search in 3 different frequencies. It is going to be considered the worst case for Synchronization (obtained only at last channel). For the Acquire Transmission parameters, it will be considered that each message is spaced between 2 frames. The time between the steps of Network Entry will be 2 frames and the time between a request and a response will be 1 frame.

The first step in the Network Entry process is the scanning and synchronization. Assuming that is needs to check 3 channels to get synchronized, and the search in a single channel must take 3 frames, in this step it will be spend **300 ms to get synchronized**. Then it will proceed to the **acquisition of transmission parameters**. Here, the SS must received 4 messages (DL-MAP, DCD, UCD and UL-MAP) which are assumed that are spaced in 20 ms interval. So, for this step **80 ms** are spent. Since is considered a Fixed WiMAX system, the **initial ranging** process consists in the exchange of 4 messages which makes a total of **70 ms** (40 ms for message transmission + 30 ms for interval between the request and the response). For the **Basic Capabilities Negotiation** process is spend **30 ms**. Since Fixed WiMAX was chosen, the **authorization** step takes **50 ms**[5]. Finally, the **registration** process takes

[5]The time that is requirer to interpretation the contents of the authorization messages (PKM messages) is

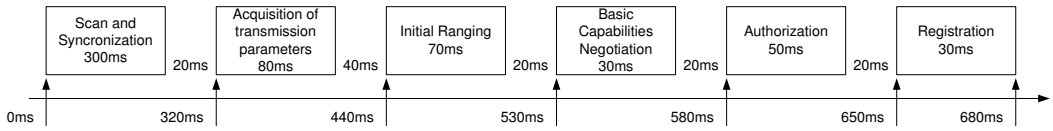

Figure 4.3: Network Entry example time analysis

30 ms. In figure 4.3 is represented the several steps and the time that is spend in each one.

Considering the parameters that are described on the table 4.1, it can be concluded that the Network process entry takes 680 ms. This time can increase if dynamic service flows are wanted. For example, if it is pretended to establish 2 service flows, and to consider the parameters described on table 4.1 and the message flows in figure 4.1, the network entry time can be 790 ms. In a real scenario, specially in a non fixed scenario, the time that is spent for scanning and synchronization, to acquire transmission parameters and for initial ranging must be higher. For example, the initial ranging process may need to exchange more messages than those represented in figure 4.2, which leads to a significative increase of time.

4.3 Network entry in vehicular communication

For a road safety vehicular communications scenario, each second that is lost in communications represents a delay in giving a safety message to the driver, which causes more distance travelled before he/she gets the knowledge of the danger. The first step that OBU needs to be executed is to get connected to the RSU and so be allowed to receive messages (network entry). During this process, it is not possible for the OBU to receive or transmit data, so no safety messages can be received during this. This is a subject that is needed to be taken into account when projecting a V2I/I2V system. In the WiMAX network entry example present above, it is spent about 1 s to SS become ready to receive/transmit data. Assuming a vehicle at 250 km (exaggerated velocity nowadays for a road vehicle), this means that a vehicle travelled approximated 70 m before receiving any message. The relevance of the distance that is travelled during the network entry process is related to the percentage of that distance in the coverage area. If a RSU coverage area is 3 km, a typical value for WiMAX coverage [JGA06], 70 m represents a small part of that. Of course, it is also need to take in account the reaction time of the driver and the vehicle stopping distance [Gro08], in order to supply an effective safety service. Considering the vehicle velocity equal to 250 km, and assuming the mean reaction time of a person, 0.8 s [Gro08] (implies 56 m), and the stopping distance for this velocity equal to 570 m [Gro08], the vehicle takes additional 626 m to stop. It must be highlighted the high value of stopping distance because of the high velocity that has been chosen for the example[6].

One of the biggest challenges that can take a very high impact in the network entry process, and also in maintaining a wireless link, is the transmission medium. The wireless communication systems are based on complex radio wave propagation mechanisms to over-

not define in the scope of IEEE 802.16 standards [IEE04]

[6]For a velocity of 120 km, the stopping distance is approximated 180 m [Gro08]

come some setbacks like the obstructions, terrain undulations, relative motion between the transmitter and the receiver, interference from other signals, noise, and various other complicating factors together weaken, delay, and distort the transmitted signal in an unpredictable and time-varying fashion [JGA06]. Steps like synchronization and initial ranging are very sensitive to the changes in the transmission medium and can have a deep impact in the time of the network entry process. Next, it will be presented some aspects that must be taken into account for the wireless transmission medium [JGA06]:

- *Distance-dependent decay of signal power*: The received signal power typically decays with distance - pathloss. That can be aggravate with several factors like terrain, foliage, obstructions, and others;

- *Blockage due to large obstructions*: Large obstructions, such as buildings, cause localized blockage of signals. Radio waves propagate around such blockages via diffraction but incur severe loss of power in the process - shadowing;

- *Large variations in received signal envelope*: The presence of several reflecting and scattering objects in the channel causes the transmitted signal to propagate to the receiver via multiple paths. This leads to the phenomenon of multipath fading, which is characterized by large (tens of dBs) variations in the amplitude of the received radio signal over very small distances or small durations.

- *Intersymbol interference due to time dispersion*: In a multipath environment, when the time delay between the various signal paths is a significant fraction of the transmitted signal´s symbol period, a transmitted symbol may arrive at the receiver during the next symbol period and cause ISI[7].

- *Frequency dispersion due to motion*: The relative motion between the transmitter and the receiver causes carrier frequency dispersion called Doppler spread. Doppler spread is directly related to vehicle speed and carrier frequency and typically leads to loss of signal-to-noise ratio (SNR) and can make carrier recovery and synchronization more difficult, with an highlight for OFDM systems.

- *Noise*: Additive white Gaussian noise (AWGN) is the most basic element present in any communication channel and it is related with bandwidth. The higher noise floor, along with the larger pathloss, reduces the coverage range of systems.

- *Interference*: Sharing the spectrum availability with other users cause signals from different users to interfere with each other.

It is important to refer that WiMAX, in the mobile version, defines mechanisms that allow handover between several base stations, without losing the link, which implies a fast reconnection/rentry trough BSs. This implies that the MS start scan for other BS when it is still connected. In WiMAX, as in all cellular systems, the handover is performed at Layer 1,

[7]In OFDM scheme, the introduction of CP can complete eliminate the ISI [Pap08a]

2 and 3 [JGA06]. Although WiMAX define mechanisms for handover, there isn´t define the complete process execution. A big effort is this area is employed in order to develop effective mechanisms to reduce the handover time, as show by [RR06] and by [PB07]. Although is not objective of this work to study this handover mechanisms, this is a important reference because that introduces the possibility to coverage a potential road safety area with multiple BSs, without losing the link between the OBU and the RSU.

Chapter 5

WiMAX Development Platforms

5.1 Introduction

A V2I communications scenario, like the one mentioned in chapter 1, requires the existence of a RSU (fixed infrastructure) and a OBU (vehicular platform). Using WiMAX technology for that propose can easily be match the RSU to a WiMAX BS and the OBU to WiMAX SS (or MS), this in a PMP topology. The RSU is responsible to control the medium access (MAC control) and to transmit information (safety or non safety data) to all OBUs that are connected to it. In other way, the OBU have to detect and connect to the RSU to receive that information data. WiMAX technology is totaly orientated to perform a bidirectional communication so, the OBU can easily send information to the RSU (warning messages, requests for additional data, etc.).

In this work, is pretend to study the the real-time performance of WiMAX in order to perform road safety communication (e.g. warning messages) and the coexistence of safety (more priority) and non-safety (less priority) communications, taking part of WiMAX QoS at MAC layer. For that, it necessary to have access to WiMAX equipments. The WiRia project, here the author is currently working, provided that access to the WiMAX equipments. It is important to say that WiRia project was the main support for this thesis. Like has mention in chapter 1, WiRia project objective is to develop a fixed WiMAX SS. To get that objective, it was performed a study of development platforms for Fixed WiMAX, to get the knowledge of the features of development boards present in the market and to choose one development board. This study is present in a section bellow. In the ambit of WiRia project, it was also available (in a partial time) a WiMAX FORUM certified BS and SS, from Redline Communications, Inc [Com07a].

5.2 Market Study of WiMAX Development Platforms

The WiRia project orientation was to find a development platform which can allow to develop a compliant Fixed WiMAX SS and, to a possible future line of work, develop a Fixed WiMAX BS. There has been consider several points of study like the standard compatibility and certification (IEEE 802.16-2004, IEEE 802.16e-2005 or both), the type of device that can

Figure 5.1: ASPEX WiMAX development kit, from [Sem07]

be developed (SS, BS or both), the duplex mode allowed (FDD, TDD, H-FDD), the available bandwidth, the operation frequency, the platform structure (access type, modularity, ...), the quality of the developing tools (free or proprietary, price, royalties fees, ...), the manufacturer support and other specific aspects of each platform. Next, a brief overview of each platform studied is presented, followed by a comparison between them.

5.2.1 ASPEX WiMAX Development Kit

The ASPEX semiconductor company provides a WiMAX development kit (figure 5.1) that can be used to develop solutions according to both IEEE 802.16-2004 and IEEE 802.16e-2005 standards [Sem07]. It consists of a Peripheral Component Interconnect Extended (PCI-X) plug-in card (Accelera 3000) containing Aspex's Linedancer processors, reference software for the IEEE 802.16-2004 and 802.16-2005 PHY, and an integrated MatLab test-bench environment.

The Aspex WiMAX PHY reference code implements all the mandatory features of the IEEE 802.16-2004 and 802.16e-2005 PHY, and also supports optional features such as sub-channelization and multi-antenna options, enabling initial infrastructure deployments. This reference code runs under Linedancer Extreme Processor which is a fully software programmable, ultra-high performance processor that implements the Aspex Associative String Processor (ASP) architecture.

Despite of implementing all the mandatory features for the WiMAX PHY, this development kit doesn't have a radio board nor any code for the MAC. There is also a lack of information about most of the aspects that are considered relevant in this market study.

5.2.2 FUJITSU WiMAX Reference Kit

Fujitsu Microelectronics company provides a WiMAX Reference Kit (figure 5.2) that uses the Fujitsu MB87M3550 System-on-Chip (SoC), which implements the PHY and part of MAC according to the IEEE 802.16-2004 standard [Ame07]. This development board can be used to build SS and BS (using an external processor) solutions allowing TDD or H-FDD duplex mode supporting up to 7 MHz of bandwidth (despite of the 20 MHz available from the SoC).

Figure 5.2: Fujitsu Fixed WiMAX development kit, from [Ame07]

The MB87M3550 SoC has three embedded parts that execute the PHY and MAC functions: (1) a baseband hardware blocks that execute the OFDM PHY functions; (2) an ARC processor that implements the Lower MAC (LMAC) functions such as cyclic redundancy check (CRC) calculation and encryption of data (firmware provided by Fujitsu); and (3) an ARM processor that performs all the Upper MAC (UMAC) functions (object code, SS version only). Therefore, this SoC only allows the development of the UMAC layer functions. It also includes some integrated peripherals like UART/RS-232 interface, I2C interface, SPI interface, a radio interface and two independent debug ports (ARM and ARC). The development kit includes a radio module that interface with the SoC (3.4 - 3.5 GHz), a network and RS-232 interfaces and on-board memory (RAM and Flash). The UMAC functions run under VxWorks real-time operating system and the development tool will be Tornado IDE from WindRiver [Riv07].

The development platform from this manufacturer have the necessary requirements to project WiRia because it already implements the RF stage (using a radio module), the PHY and lower MAC functions of WiMAX giving the possibility of implementing and controlling the upper MAC functions using the development tools associated with VxWorks. It have the disadvantage of the royalty feeds of the Real-Time Operating System (RTOS) VxWorks and tools associated.

5.2.3 INTEL WiMAX System-on-Chips's

Intel company provides two different SoC's to develop WiMAX solutions: Intel WiMAX Connection 2250 and Intel PRO/Wireless 5116 BroadBand Interface [Int07]. These SoC's are very similar and the main difference between them is that the first one can be used to develop fixed and mobile WiMAX solutions and the second one only supports Fixed WiMAX solutions.

The Intel WiMAX Connection 2250 is compliant with both IEEE 802.16-2004 and IEEE

Figure 5.3: Sequans WiMAX development kit, from [Com07b]

802.16e-2005 specifications. The dual-specification support is enabled by a software-configurable modem that operates as an OFDM 256 PHY (for IEEE 802.16-2004 mode) or an OFDMA PHY (for IEEE 802.16e-2005 mode). It has two integrated ARM 946E-S processors that support all MAC and PHY functions allowing a channel bandwidth up to 10 MHz and TDD or H-FDD duplex modes. Some of the MAC functions implemented are PHS, Packet CS sub-layer, QoS, ARQ, HARQ, etc. It also provides RF, Ethernet, SPI, memory (SDRAM and flash) interfaces. The Intel PRO/Wireless 5116 BroadBand Interface is similar to the SoC presented before with the exception of the PHY layer which is not programmable and only OFDM 256 PHY can be used. It is important to mention that these two SoC's are compatible, that is, the package and the pin layout are the same and therefore solutions that uses Intel PRO/Wireless 5116 Broadband interface are easily adapted to the Intel WiMAX Connection 2250.

These two SoC's have good characteristics to be used in this project but the lack of information about a development kit that implements the SoC necessary hardware is a serious limitation.

5.2.4 SEQUANS WiMAX Development Boards

Sequans Communications company provides two different development boards (figure 5.3) that can be used to build SS and BS solutions, respectively, using SoC's from this same manufacturer [Com07b]. The SQN1010-RD board (SQ1010 SoC) can be used to develop SS solutions while the SQN2010-RD (SQN2010 SoC) board is directed to BS solutions.

The two SoC above mentioned are quite similar, they both implement all the mandatory functions of the IEEE 802.16-2004 PHY and PHY allowing up to 28 MHz of bandwidth and TDD, FDD or H-FDD duplex mode. The main difference between them is the inclusion of an extra ARM 9 processor in the SQN2010 SoC because it is targeted to BS development, thus requiring more processing power. They implement PHY features like robust synchronization, uplink sub channelization and MAC features such as PHS, ARQ, privacy (DES and DES) and packet CS. Sequans deliver full software package with hardware drivers, MAC and scheduling functions running under Linux or VxWorks.

The SQN1010-RD and SQN2010-RD Reference designs are platforms that demonstrate the capabilities of Sequans' SQN1010 and SQN2010 SoC´s and full software package. These

two boards can work in two different modes: RF mode using third party RF module or Intermediate Frequency (IF) mode using IF boards provided by Sequans. They also have some peripherals like flash and RAM memory, Ethernet and serial transceivers and interfaces such as RJ-45, JTAG or RF.

The development tools from this manufacturer have good features and thus, are a good possibility to be used in this project. It is important to mention that these two development boards and associated SoC's are certified by WiMAX Forum. However, one of the drawbacks presented is the unavailability for supply an RF board and the necessity to use different SoC's to implement SS or BS solutions.

5.2.5 TELECIS WiMAX Development Board

TeleCIS Wireless company provides the TCW 1620 SoC and a development board that allows the implementation of fixed/portable WiMAX solutions [Wir07].

The TCW 1620 SoC supports both PHY and MAC layers according to the IEEE 802.16-2004 standard providing Ethernet, PCI and RF interfaces and supporting up to 20 MHz of bandwidth with low power consumption (< 350 mW). It implements MAC features such as packet classification, QoS, ARQ, PHS and AES/DES security and PHY characteristics like dynamic frequency selection. This manufacturer has a Reference Design Kit, using the TCW 1620 SoC, that is fully functional and support easy customization via Web-based user interface pages supported by an on-board Hypertext Transfer Protocol (HTTP) server. TeleCIS also provide a BS emulator board capable of connecting to SS developed solutions with limited functions.

The SoC provided by this company have the necessary features to be considered in this project, however, the lack of more detailed information about specific characteristics from the development board is a major drawback.

5.2.6 Wavesat WiMAX Development Solutions

Wavesat company has a set of products that can be used to develop WiMAX solutions (figure 5.4): an Application-Specific Integrated Circuit (ASIC) that implements the PHY layer, a MAC Coprocessor that performs lower level MAC functionalities and MAC software running on a specific processor [Wav07]. Using the products described, Wavesat created several development boards that can be used to speed up WiMAX solutions construction.

The Evolutive DM256 ASIC implement the IEEE 802.16-2004 OFDM PHY. In the transmission process, it receives a digital signal and gives a baseband or IF (up to 20 MHz) analog signal (performs the inverse process when receiving). It allows up to 10 MHz of bandwidth, supports TDD, FDD and H-FDD duplex mode and can be used in SS or BS solutions. The MC236 MAC Coprocessor implements the low-level MAC functionalities and its purpose is to be a companion of the DM256 ASIC. It provides a bridge between the DM256 ASIC and the processor used to perform MAC operations offloading from it timing-critical operations (decoding DL-MAP and UL-MAP, CRC and header check sequence (HCS) calculation, encryption, ...). It is also provided software (source-code) for a WiMAX SS MAC tested with

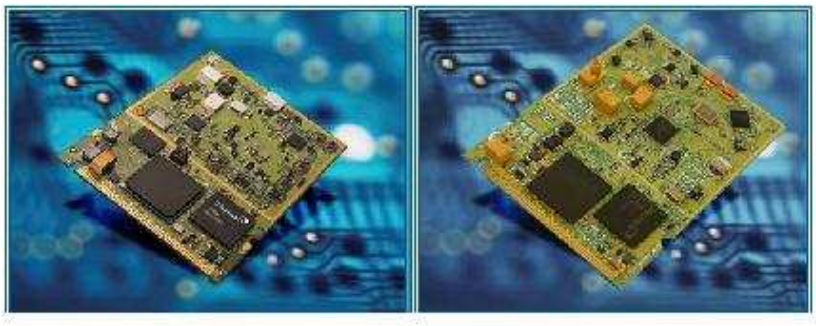

Figure 5.4: Wavesat WiMAX development kit, from [Wav07]

---

the Intel Xscale IXP425 running on Linux OS. It conforms to the IEEE 802.16 standard and is meant to be used with the DM256 ASIC. It implements all the mandatory features from WiMAX and optional ones like ARQ, PHS and UL sub-channelization.

Some of the development boards provided by Wavesat only implement the RF stage, PHY processing using the DM256 ASIC and the lower MAC functions using the MAC Coprocessor. There are two different designs depending on the RF frequency desired: 3.3 - 3.8 GHz and 5.150 - 5.875 GHz. WaveSat has another board that interfaces with the two previous ones implementing the MAC functions using the xScale IXP425 Intel processor running the MAC software previously mentioned. Therefore, Wavesat provides a complete WiMAX solution implementing all the MAC, PHY and RF processes needed by an SS.

The solutions from this manufacturer has to be considered because they present good characteristics to the purposes of this project. They provides a complete WiMAX solution and have modularity and therefore each part can be used as stand-alone enabling the development of own hardware.

5.2.7 Comparison of WiMAX development platforms

After describing all the development platforms and respective manufacturers studied, a comparison between all of them was done in order to justify the choice made for WiRia project. The WiMAX plataforms comparison can be seen in table 5.1 and it is followed by the development platform choice justification.

Analyzing table 5.1 it is possible to see that the INTEL company doesn't provide a development board. That is an unsurmountable drawback because time requisition and it is not an objective to develop all the necessary hardware in the WiRIA project, so, this manufacturer products has been considered for this project. All the other companies provide development platforms that can be used to speed up a final solution. However, ASPEX company development board has was discarded because it doesn't implement any MAC functions nor any base to develop them which is a serious drawback also due to project time limitation. The other development boards implement all the mandatory functions of the PHY and MAC but, despite of that, only FUJITSU and Wavesat will be considered because only their solutions implement the RF stage, which was a major requirement in the study because in WiRia

Manufacturer	ASPEX	FUJITSU	INTEL	SEQUANS	TELECIS	WAVESAT
Products available	PHY on Linedancer Processor	SoC with PHY and MAC integrated	SoC with PHY and MAC integrated	SoC with PHY and MAC integrated	SoC with PHY and MAC integrated	ASIC with PHY, CoProcessor with LMAC and Processor with UMAC
Development Board	YES	YES	NO	YES	YES	YES
Standard Compatibility	802.16-2004 802.16e-2005	802.16-2004	802.16-2004 802.16e-2005	802.16-2004	802.16-2004	802.16-2004
Type of device that can be implemented	SS or BS	SS or BS (using external processor)	SS or BS	SS or BS	SS	SS
RF Board	NO	YES (3.4-3.5 GHz)	NO	NO (only IF)	NO	YES (3.3-3.8 GHz and 5.1-5.8 GHz)
PHY Layer	OFDM and OFDMA	OFDM	OFDM and OFDMA	OFDM	OFDM	OFDM
MAC Layer	NO	YES (Code running under VxWorks)	YES	YES (Code running under VxWorks or Linux)	YES	YES (Code running under Linux)
Duplex mode available		TDD or H-FDD	TDD or H-FDD	TDD, FDD or H-FDD		TDD, FDD or H-FDD
Bandwidth available		20 MHz (Development board limited to 7 MHz)	10 MHz	28 MHz	20 MHz	20 MHz

Table 5.1: WiMAX development platforms comparison

project was pretended to acquire a development board which can supply a full equipment solution (project hardware to interact with the PHY of several SoCs/glsasic wasn´t pretend).

So, the only companies that provides products that fulfill the requirements for this project were FUJITSU and Wavesat and therefore one of them was chosen. The development platform chosen was FUJISTU's due to the next factors: it presents a much more integrated solution using a SoC that implements all the PHY and MAC functions (but it is possible to develop our own upper MAC functions interacting with the lower MAC firmware), this SoC can be used to develop SS and BS solutions (which is a future objective in the WiRia project) and the fact that FUJITSU has already test their solution with the commercial Redline Communications BS (same equipment available in WiRia project).

5.3 Commercial WiMAX equipments

In the market there several manufactures of Fixed WiMAX equipments, like Alvarion [Alv07], Aperto Networks [Net07b], Airspan Networks [Net07a], Redline Communications [Com07a],

Figure 5.5: AN-100U, Redline Communications Base Station, adapted from [Com07a]

---

and many others. The objective of this section is not to present a market study about Fixed WiMAX equipments, but to describe some features of the equipments that was used to perform WiMAX tests to evaluate the use of WiMAX for V2I communications, more specific, the AN-100U (Redline Communication BS) and the SU-O (Redline Communication SS).

5.3.1 Redline Communications BS - AN-100U

The AN-100U unit is a Fixed WiMAX compliant wireless BS for deployment of PMP and point-to-point (PtP) systems (figure 5.5) [Com07a]. It consists of an indoor terminal (Indoor Unit (IDU)) and outdoor transceiver and antenna (Outoor Unit (ODU)). This BS is designed to work in the frequency range of 3.4 - 3.6 GHz with a bandwidth of 3.5 or 7 MHz. The PHY layer is based on an OFDM transmission scheme with an FFT of 256 points using a TDD scheme to transmit and receive on the same channel. It provides the mandatory modulation (BPSK, QPSK, 16QAM and 64QAM) and coding rates (1/2, 2/3, 3/4) and implements rtPS and BE IEEE 802.16-2004 QoS service classes. The IDU unit provides the implementation of IEEE 802.16-2004 MAC and PHY and interfaces to manage the equipment, via Ethernet Port or serial Port. The ODU is constituted by an RF transceiver and an antenna. The RF transceiver receives the IF signal coming from the ODU along with some control signals and sends an RF signal to the antenna. The maximum transmission output power allowed is 23 dBm and the antenna has a directionality of 90^o providing an extra gain of 14 dBi.

5.3.2 Redline Communications SS - SU-O

The SU-O WiMAX SS is a Fixed WiMAX compliant for PMP and PtP deployments (figure 5.6) [Com07a]. It provides connectivity with a WiMAX BS using an operation frequency of 3.4-3.6 GHz and an OFDM transmission scheme with a channel bandwidth of 3.5 or 7 MHz. It provides communication using a TDD or an H-FDD using all mandatory modulation (BPSK, QPSK, 16QAM and 64QAM) and coding rates (1/2, 2/3, 3/4). The SU-O

Figure 5.6: SU-O, Redline Communications Subscriber Station, from [Com07a]

---

consists in an ODU that comprises all the RF, PHY and MAC processing as well an integrated antenna and an IDU that consists in a Power over Ethernet (PoE) module. The PoE module has an Ethernet interface, for connecting to customer equipments receiving traffic, and an AC power interface, for provide power to the ODU through another Ethernet interface. The users' traffic is also transported in this Ethernet interface. In this SS, the maximum transmission output power allowed is 20 dBm and the antenna has a directionality of 15º providing an extra gain of 14 dBi.

Chapter 6

Building a Fixed WiMAX Subscriber Station

6.1 Introduction

It is a requirement to have the knowledge of the WiMAX MAC and PHY key features in order develop any WiMAX equipment (whether a SS/MS/CPE or whether a BS). For the Fixed WiMAX, this key features includes a MAC management layer, service-specific CS, privacy, authentication (and key-management services), PHY setup and control, PSAP management, the PSAP scheduler, data control processor, OFDM PHY driver and all available Access Point Interface (API)s to this several parts [Zee07]. Like was show in chapter 5, each WiMAX SoC manufactures has its own approach to implement those parts. It is important that all MAC and PHY features are encapsulated and be accessible to upper layer through high level data and management APIs. Another important feature is to have the ability to interconnect this WiMAX module to the services that are wanted to include in the final system. One of the most common, in data plain, is to interconnect an Ethernet interface to the WiMAX module. The RF system part have a special relevance, and this have to be projected in concordance to the final objective of system.

This chapter presents a detail description of the WiMAX development board chosen for the WiRia project, Fujitsu Fixed WiMAX Reference Kit, to implement a Fixed WiMAX SS. Here aspects like hardware and software architecture will be addressed. Then, it will be present the work that have be done in order to transform the development kit to a commercial SS, with the requirements of WiRia project.

6.2 Fujitsu Fixed WiMAX Reference Kit

Fujitsu´s Fixed WiMAX Reference Kit (show in chapter 5 figure 5.2) provide to developers the design and the environment to test key aspects of a Fixed WiMAX implementation, drawing the features of Fujitsu MB87M3550 802.16-2004 SoC [Ame06b]. This SoC provides the implementation of Fixed WiMAX PHY processing (OFDM PHY) and several lower MAC functions in order to develop a compliant equipment with WiMAX FORUM specifi-

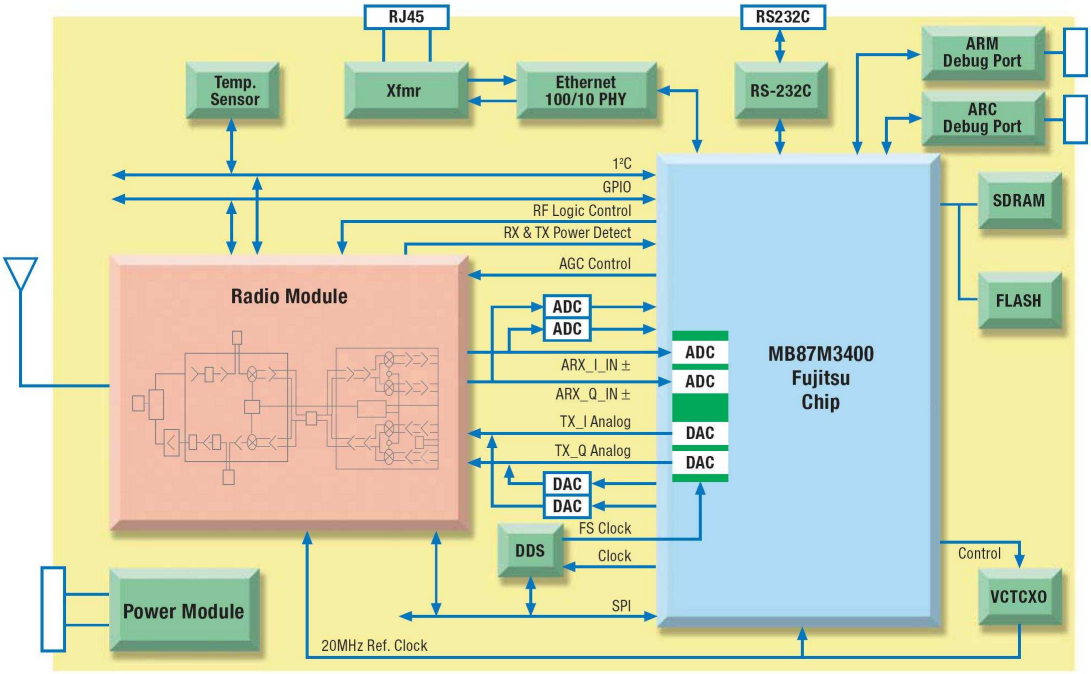

Figure 6.1: Fujitsu Fixed WiMAX reference kit, from [Eur07]

cations [Ame06a]. The reference kit can be configured to support either TDD or H-FDD, depending on the radio selection. Additional, is supplied a software package to install the reference kit as a WiMAX SS.

6.2.1 Hardware Architecture

Overview

In figure 6.1 is represented the Fujitsu Fixed WiMAX reference kit hardware architecture, in internal processor mode[1]. The Fujitsu´s SoC can operate in two differents mode: internal or external processor mode. The difference between then is that in internal mode the full WiMAX MAC must be implemented on the SoC. In external mode, the SoC only process low-level WiMAX MAC functions, LMAC functions, and allow the UMAC functions be executed in an external processor (that allows more processing capacity). The external processor mode is important for the implementation of high performance SS or a high capacity BS (support an high number of SSs). Fujitsu´s reference kit allow the addiction of a external processor board. However, that it is not described because the orientation of this work (and WiRia objective) is to build a SS that use the software package for WiMAX SS supplied by Fujitsu, which only runs in internal processor mode.

[1]In figure 6.1 is represented the Fujitsu reference kit hardware architecture using an older version of Fujitsu´s SoC (MB87M3400). However, the use of the SoC (MB87M3550) don´t introduces any change to the high level architecture.

The Fujitsu WiMAX reference kit is designed to support the SoC features and interfaces. The key features of the reference kit board is [Ame06b]:

- RF port interface for third-party radio;
- Radio module from SiGe Semiconductor [Sem08](for 3.4-3.5GHz operation and 3.5MHz bandwidth);
- Network interface (Ethernet PHY and RJ-45 interface);
- On-board memory (128Mbits Synchronous Dynamic Random Access Memory (SDRAM); 64Mbits Flash)
- On-board peripherals control using Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I^2C) and General Purpose Input/Output (GPIO)
- On-board Voltage Controlled Temperature Controlled Crystal Oscillator (VCTCXO) for Automatic Frequency Control (AFC) mechanism;
- On-board Direct Digital Synthesis (DDS) for baseband signal analog-to-digital converter (ADC)s and digital-to-analog converter (DAC)s;
- Debug port interfaces;
- RS232C interface port;
- External power supply interface.

MB87M3550 SoC

As referred before, the MB87M3550 SoC can be view as an integrated WiMAX MAC and PHY signal baseband processor, and is the main element of the reference kit. In figure 6.2 is represented the block diagram from this SoC. Where, three blocks must have to be distinguish:

1. *OFDM PHY* - provides the baseband PHY signal process, which supplies and receive the baseband signal to/from a external RF board, using internal ADCs and DACs. This supports bandwidth channels from 1.75MHz to 20MHz and efficient adaptive modulation schemes, including 64QAM, 16QAM, QPSK and BPSK, which allow the SoC´s data rate go up to 75Mbps [Ame06a]. Automatic Gain Control (AGC) feature supported by the SoC can be view as a integrated part of this subsystem;
2. *LMAC Reduced Instruction Set Computers (RISC) Engine* - based on ARC Tangent RISC architecture, implements the IEEE 802.16 LMAC functionalities, such has encryption/decryption (DES/AES) engines and a CRC checker/inserter. It also supply the some features, like the CID search mechanism, in order to improve the MAC performance;

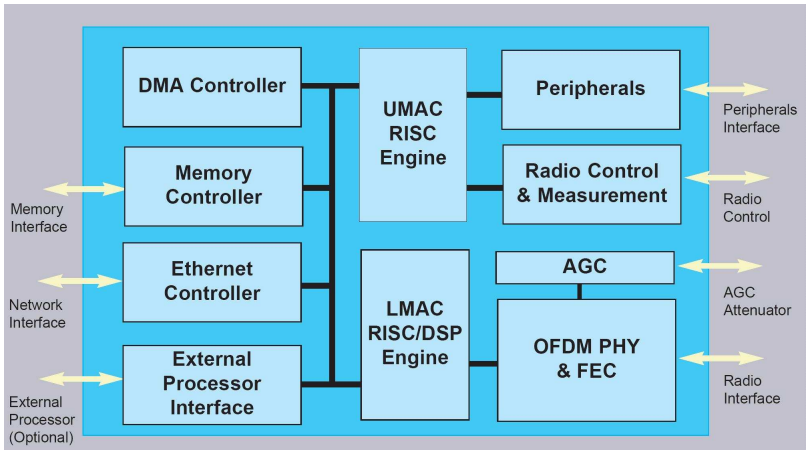

Figure 6.2: Block Diagram of Fujitsu Fixed WiMAX SoC, from [Ame06a]

---

3. *UMAC RISC Engine* - based on ARM 926 RISC architecture, implements the IEEE 802.16 UMAC, Device Drivers, Protocol Stacks, and User Application software. It is responsible for control the data and control communications between LMAC, as so, the reference kit peripherals control.

The three blocks present above are the core elements of the SoC. The LMAC part allows the encapsulation of all interaction that the WiMAX MAC needs to perform with the WiMAX PHY. This means that, UMAC developers are completely abstraction of PHY interface. At WiMAX point of view, UMAC processor communicate only the LMAC processor, where PSAP is provided by this last processor. The communication between this two MAC processors can be accelerated using the multi-channel Direct Memory Access (DMA) present in the SoC. This DMA can also be use to improve communications for memory controller and Ethernet Controller. The memory controller allows the interface for external SoC SDRAM and Flash memory. The Ethernet Controller provides the access for a external Ethernet PHY and implements the Ethernet MAC. The UMAC engine is also responsible to control the several peripherals present on the reference kit, such as DDS control by SPI interface, the VCTCXO control by a internal DAC or the RS232C interface.

6.2.2 Software Architecture

Before describe the software architecture of MB87M3550 SoC, included on Fujitsu Fixed WiMAX reference kit, is important to refer that: the OFDM PHY can´t be modified/upgraded because of its fixed implementation of hardware blocks and registers; the LMAC subsystem executes a firmware supplied by Fujitsu; and the UMAC subsystem runs software that can be developed, which is normally associated with a RTOS. Fujitsu supplies several versions of LMAC firmware, where the choose depends of the objective of the system (SS or BS). Figure 6.3 shows an overview of Fujitsu's software architecture. The several blocks present in this figure, all runs on the UMAC engine (ARM core) except the 802.16 LMAC, which runs

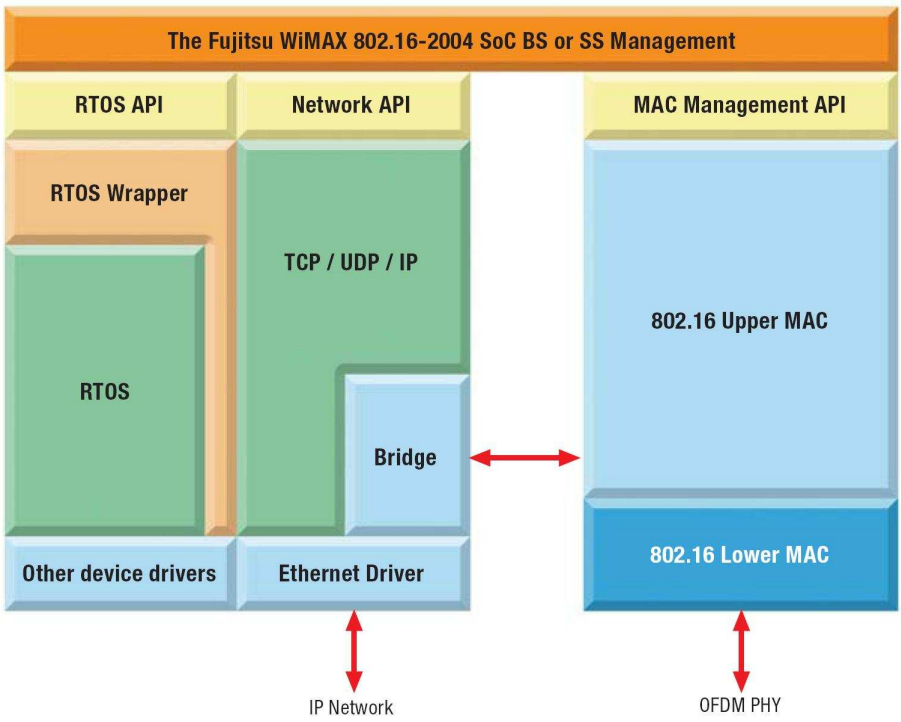

Figure 6.3: Overview of Fujitsu Software Architecture, from [Eur07]

---

under the ARC Tangent core. However, this architecture is the one proposed by Fujitsu and used in its SS software package. For UMAC developers, is available mechanism to LMAC communication, based in memory mapping and interrupts, which is architecture independent and allow developers to builds its own solution totally free from the architecture present in figure 6.3.

Fujitsu WiMAX SS software package

As referred before, Fujitsu supply a software package that allows to implements a Fixed WiMAX SS on Fujitsu's MB87M3550 hardware reference platform. The software package is the LMAC firmware and the image/modules of the UMAC, where is presents the follow elements:

- 802.16-2004 MAC (includes UMAC and LMAC) Library and API;
- Routing 802.3 Ethernet Packets - MAC Bridge;
- System Configuration Manager Library and API;
- Radio Library for SiGE WiMAX Radio and API.
- User Interface Source Code and Library;

This software package allows the reference kit to operate as WiMAX SS for a bandwidth of 3.5MHz, a frame duration of 10ms, CP length equal to 16, all coding rates and burst profiles as per IEEE 802.16-2004, support two of QoS classes defined in IEEE 802.16 standard: BE and rtPS; and provide a IEEE 802.16 CS for Ethernet, virtual local area network (VLAN) and IPv4. Those features have been tested (by Fujitsu) in a scenario here the reference kit was connected to Redline BS (AN-100U)[2].

Fujitsu WiMAX SS software package runs under VxWorks RTOS, from Wind River [Riv07]. VxWorks, based on a multitasking kernel, uses a scheduling algorithm based on fixed priorities, that is, the task which has the higher priority and that is ready to run is the one that takes the processor. For same task priority, the scheduling algorithm can be frist-in, frist-out (FIFO) or Round Robin. Fujitsu also provides for this RTOS the Board Support Package (BSP), which includes, for example, the several peripherals device drivers (e.g. Ethernet or SPI) or the interruption vectors of the system. The LMAC interface isn´t supplied by the this BSP, as so, the RF board device driver. The network stack (IP/Tansmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack) is supplied by the RTOS VxWorks, where is available several APIs for make this stack accessible by other modules (e.g. Telnet module). This network stack communicates directly to Ethernet device driver (in transmission mode) or with the MAC Bridge module (in reception mode). The MAC Bridge module in this software package is responsible for the forward of the incoming Ethernet packets to the RTOS Network Stack or to the CS of the UMAC module, based of MAC address classification. It is also responsible to receive the packets from the UMAC CS and forward that to the Ethernet Driver.

In Fujitsu´s Software Architecture, shown in figure 6.3, is presented a Management module. In the software package, this module is matched to the system configuration manager and the user interface libraries. The user interface, available by serial interface only (RS232C), allow the configuration and monitorization of the system. For that, it uses the APIs available in the other modules. The user interface module is very related to the system configuration manager module, which controls operations like system initialization or software upgrades.

6.3 Develop a Commercial SS

The objective of this section is to show the effort that was spend in WiRia project to make a final SS solution. For this solution, based in the Fujitsu WiMAX Reference Kit, was specified several requirements (mostly for management) which are going to be presented and the way to achieve that. Unfortunately, for this thesis wasn´t possible to build a totally oriented OBU unit for road safety services which possible can lead to a different software architecture than that is going to be present for the WiRia SS.

[2]This connectivity test it was also made by the author where those features was been tested successfully, excepted the VLAN CS which wasn´t tested.

6.3.1 Objectives/Pretended Features

The SS software package supplied by Fujitsu have the minimum functionalities to establish a WiMAX link and have the availability for transmission Ethernet packages through the air. However, in this software package, the management part of SS presents several limitations, special in the way to processed that (via RS232C). For the WiRia project, have an effective way to proceed SS management is one of the main objectives. It is also imperative to have the possibility to execute management through the air link. At WiMAX UMAC level, since for this part is supply by Fujitsu in object code, so no modifications are possible and the WiMAX MAC features support by the SS are those that is supplied by Fujitsu software package. Next, are presented the main features required by WiRia project for the SS (WiMAX are not referred, because is limited by Fujitsu):

- Full SS management system;
- Management through Ethernet, Serial and Air;
- Management interfaces: website and Command Line Interface (CLI);
- System Upgrade possibility;

The interfaces that are select as mandatory for WiRia project are available in Fujitsu´s reference kit hardware design (RJ-45 for Ethernet; DB-9 for serial communication; MSX for RF signal[3]). However, some changes have to be performed in the reference kit hardware design, like the removal of several debugging components or the rearrange of the components.

6.3.2 Software architecture and challenges

After defined the objectives for the WiRia SS, it was proceeded to the definition of the software architecture. The model presented by Fujitsu (figure 6.3) was redesigned in order to match the needs of the pretended SS. An overview of the new software architecture model is shown in figure 6.4. Here, two major parts have to be distinguish: The data flow between the UMAC and Ethernet, involving the Ethernet, MAC Bridge and UMAC modules; and the User Applications module. The data flow between the Ethernet and UMAC don´t involve the VxWorks network stack. In order to allow the management through the air, ie, have the capacity of access to VxWorks network layer through the UMAC side, changes have to be made in MAC Bridge and VxWorks Ethernet drivers level (explained bellow). The user applications for this SS can be view as configuration and management applications:

- *Web server* - which allows the the access to the SS management system via HTTP, either through a website or either through a sending/receinving eXtensible Markup Language (XML) files (via HTTP GET/POST messages);
- *CLI* - an advanced management interface, which allows the execution of advanced commands. Can be accessible via Serial port or via Telnet;

[3]The RF connector can easily be substituted by another type (SMA or N-Type)

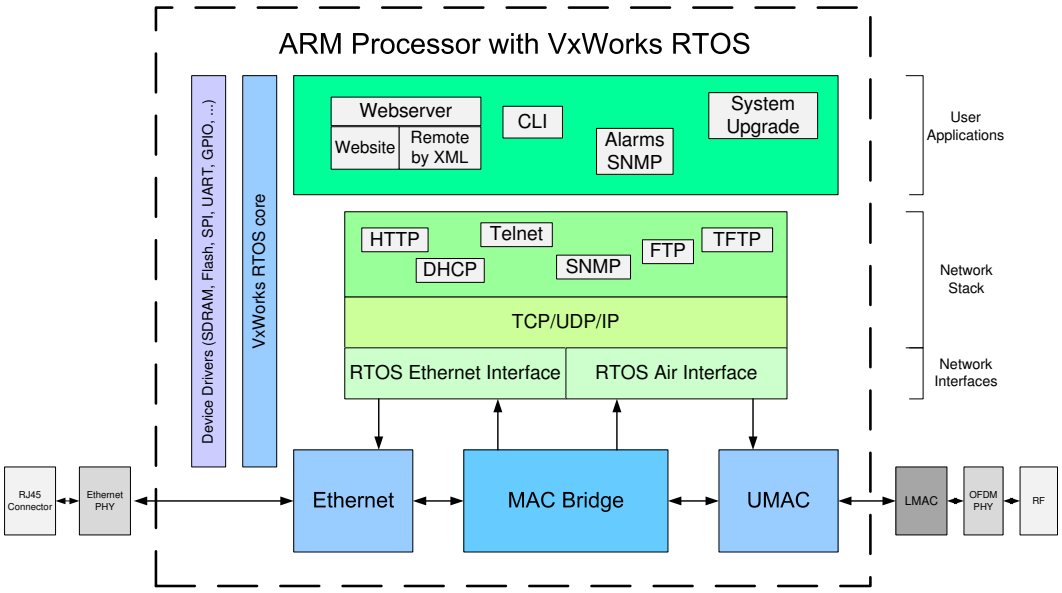

Figure 6.4: Overview of WiRia SS Software Architecture

- *SNMP* Alarms - which permit to the SS send spontaneous messages to a specific network place, in order to inform any change that occurs[4];
- *System Upgrade* - allows the exchange of the VxWorks image to upgrade the system with new features/improvements.

This user services presented above require the use of the VxWorks network stack, which supplies the full IP/TCP/UDP stack and some network application layer protocols (Telnet, File Transfer Protocol (FTP), TFTP and part of DHCP). Additional protocols, like the HTTP or SNMP, have to be implemented.

In the Fujitsu SS software package is available a management module, which allows the management of the RTOS, network and UMAC modules. After a few tests to this management module it was concluded that this module for RTOS and network management is not satisfactory for WiRia SS. One example of this is: using the management module supplied by Fujitsu, change the IP address of Ethernet interface requires a system reboot, but the VxWorks system supports this change in real-time, without the need of reboot. The UMAC part, as referred before, is a closed part, so any change is not allowed. One important feature that this UMAC doesn´t support is the secondary management connection, defined as optional in the IEEE 802.16 standard [IEE04]. The secondary management connection allows SS management traffic pass through the air, which is a requirement for WiRia SS. To circumvent this limitation, a mechanism was developed to allow air management traffic to the SS.

[4]The SNMP alarms module must be not confused as a SNMP agent

6.3.3 Functional Description

In the software architecture described above presents several changes and new features that had be implement on the WiRia SS. The objective of this part is to described the way that was choose to resolve it.

System network interfaces

As referred before, one objective that was pretend to the SS is to manage it through the air. Except the CLI using the serial interface, all management user interfaces depends of the network stack. So, allow simultaneous management through the Ethernet interface and through the air, the VxWorks network stack need to see two physical interfaces. That has the approach used.

VxWorks network stack supports a network driver interface called the MUX [Riv03]. This interface have the objective to abstract the network upper layers (great and equal than OSI model layer 3) from the physical interface used. The MUX interface supports two network driver interface styles, the Enhanced Network Driver (END) interface and the Network Protocol Toolkit (NPT) driver interface. The Ethernet driver supplied in the Fujitsu reference kit for the Ethernet interface is END style. In its drivers, the mechanisms for hardware interaction are defined.

The network driver, as the name says, is a device driver for a physical network interface. At least, the drivers´ interfaces supported by VxWorks is totally orientated for that. The idea to integrate a new interface for air communication implies the change of that. This air interface received packets from the network stack and forward that to the UMAC module. The packets received from the UMAC side are passed to the network stack. Those are the only functions that this device driver executes, without considering initializations and configurations functions required by driver style interface. In order to integrated a new interface in the MUX layer, a template file for END network driver, supplied by Wind River, was used. Using this template was possible to build a network driver for a interface that physically don´t exists, passing through several initialization and configuration functions related with hardware interaction.

After the implementation of this new interface, the VxWorks network layer sees two separated network interfaces: one for physical Ethernet device; other for Air interface through UMAC module[5].

Internal Packets Forward

One of the most important internal functions of the system is to connect the data packets flows of the Ethernet device, UMAC module and the VxWorks network stack. Here, the MAC Bridge module, represented in software architecture (figure 6.4), have an important paper. To better understand the internal packets forward, a diagram is represented in figure 6.5. The packets from the VxWorks network drivers are send directly to the final receptor (either

[5]Additional, a *Loopback* device was added for internal redirection of packets

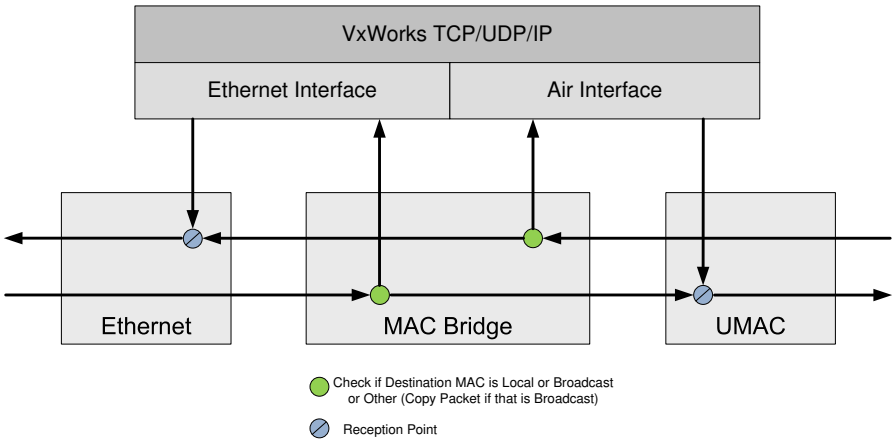

Figure 6.5: WiRia SS internal packet forward overview

Ethernet or either UMAC). The destination MAC address of packets that are from Ethernet are evaluate at the MAC Bridge and three situations can happen:

1. If destination MAC address is the Ethernet device MAC address, the packet is send to VxWorks network stack;

2. If destination MAC address is a Broadcast address, the packet is copied and forward for both VxWorks network stack and UMAC module;

3. If is not any of the cases above, the packet is send to UMAC.

On a similar way, the packet incoming from UMAC can be processed as:

1. If destination MAC address is the Air device MAC address, the packet is send to VxWorks network stack;

2. If destination MAC address is a Broadcast address, the packet is copied and forward for both VxWorks network stack and Ethernet;

3. If is not any of the cases above, the packet is send to Ethernet.

This data flow mechanism allows the communication to VxWorks network stack from Ethernet and from Air, maintaining the data flow from Ethernet to UMAC (and vice versa), which is the main packet flow of the system. However, this forward mechanism can be easily improved removing the packet copy in broadcast treatment. VxWorks network devices have associated to them a memory poll. A memory poll is pre-allocated memory, organized in pre-defined blocks size, where is allowed the reused of those blocks [Riv03]. The size of the blocks must be oriented to the final application. For a network driver, the size of the blocks is normally the Maximum Transmit Unit (MTU) size. The memory poll is organized and managed by structures (mBlk and clBlk [Riv03]) that allow the use of the same data buffer for several entities, which implies the mark of the data buffer as free only when this two

entities don´t need it any more. Instead of copy the packet, this management structures potential can be used. However, there are some problems when this is used with UMAC module. The problem is unknown, then the use of actual solution described above (packet copy).

It is important to refer that only one network device memory pool is used, the Ethernet device memory pool. Using only one memory pool allow a best dimension of that to the system requirements, and also improves the memory usage of the system. The air interface memory pool was maintain, with a small size, to avoid some possible unknown problems.

Additional, the MAC bridge module have a functionality that was introduced to resolve a problem. The problem is that on VxWorks network stack is only possible to bind a TCP/UDP port associated to a specific network interface, this means that is only possible to wait for a socket message for a TCP/UDP port if that is associated with to a pre-defined network interface. For example, a webserver bind in TCP port 80 and associated to Ethernet device, is impossible to access it through the air interface. To resolved this problem, a new MAC Bridge functionality as add when the packet come from UMAC and that is to send to VxWorks network stack:

1. If packet belongs to routing service[6], the packet is modified[7] and send to network stack through Ethernet device;

2. If not, the packet is send normally to network stack through Air device;

This mechanism allows that all TCP/UDP packets from the air interface are delivered to network stack as packets came from Ethernet device. Sending a response for this packets becomes possible because that is send based on source address of that and the VxWorks routing mechanism instruct to send it through the correct device. However, is need to change the IP source address (which is the Ethernet IP address) to the air interface IP address and recalculated all checksums again. For the final user, the packet change isn´t noticed but this introduce a delay in packet processing.

Management, Configuration and Monitoring

Global APIs module It was build a module to aggregate all configuration and monitoring APIs of the SS. The objective of that was to centralized all system APIs and become this as the only access point of system operations for the management applications. The introduction of this module simplified the management applications develop because those applications only communicates with this global APIs module. This module also makes the change of one feature in the SS independent of management application. For example, whatever change the Ethernet IP address in website or in CLI, the same set of instructions are called, thanks to this module.

[6] A "routing service" is all TCP/UDP packets

[7] Packet modify means that if the IP destination address of the packet is the IP assigned to Air END device, the destination IP is changed to IP assigned to Ethernet END device and all checksums are recalculated.

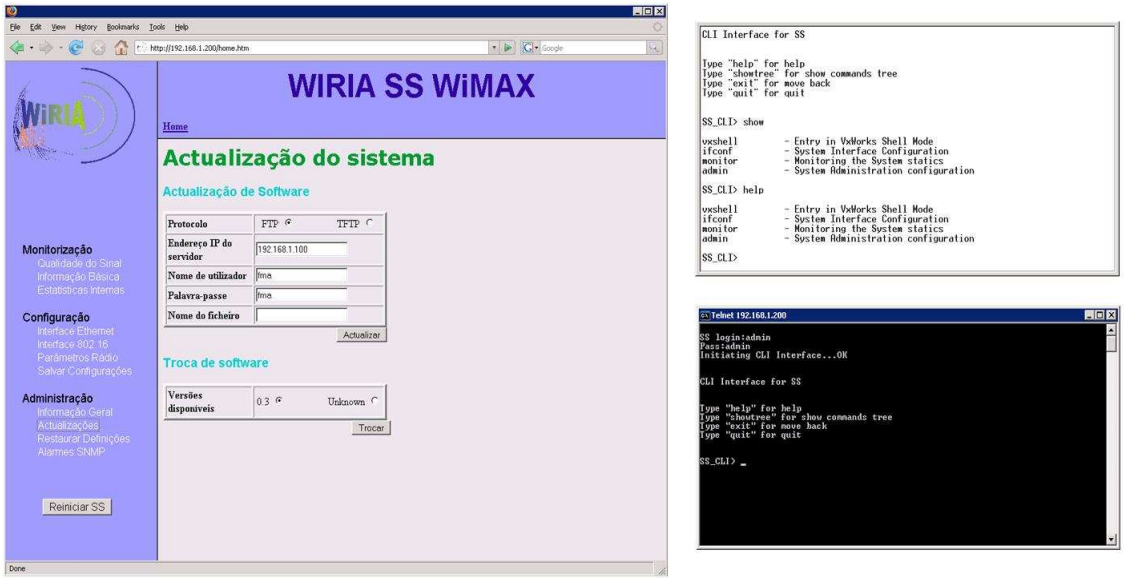

Figure 6.6: WiRia SS User Interfaces (Website and CLI)

Current and Default Configuration Files In the SS several features can be configured, like the Ethernet interface configuration or the RF board parameters. In order to allow the save of pretended system configuration (restored if system reboots), it was created a file in XML format called "current configurations". This file, saved in the Flash memory, is loaded at system initialization for load a pretend configuration. However, is it possible to restore the configurations of this files to a default configurations. The default configurations are saved in another file in the Flash, with the same format of current configurations file, that can not be changed[8]. Restoring the defaults configurations can be done by user demand or by the activation of the restore defaults pin (at the moment is a dip switch). If default configuration files don´t exists, a default values of the current image are loaded.

Web server A Web server was used to implement an user-friendly management interface, a website which was a mandatory requirement for WiRia project. First, it was made a research in order to find solutions that can allow fast time to final objective, Web server implementation. For this, it was used a Web server from GoAhead Software [Sof07], which is oriented to embedded systems. This uses Active Server Pages (ASP), embedded JavaScript, and in-process Common Gateway Interface (CGI) forms processing to deliver highly efficient and effective dynamic Web page creation [Sof07]. This features allows the used of system APIs in Web pages. Other important feature is the security support, based on HTTP 1.0 basic security, Secure Socket Layer (SSL) or Digest Access Authentication (DAA). For the ambit of WiRia project, just HTTP 1.0 basic security was used (login/password).

Through the website, is possible to monitor, configure and administrate the SS. One

[8] An advanced operation, only available by CLI, was added to allow the upgrade of the default configuration file

website page is represented in figure 6.6. The WiRia SS was projected to be included in a management network, controlled by a centralized management entity. To have an efficient remote management mechanism, it was used the potential of the Web server. For allow the remote management, it was choose a mechanism to exchange XML files between the SS and the management entity, via GET and POST messages of HTTP. This mechanism allows the management system to request XML files with monitoring information and the actual configuration of the system and send the a new pretended configuration and execute some SS operations, like reboot.

CLI Another user interface the was build for the WiRia SS was a CLI (figure 6.6). The CLI it was also a mandatory requirement for this SS. The CLI allows the execution of line commands to monitor, configure and manage the SS. Additional, advanced commands can be execute (e.g. change boot parameters) and execute VxWorks shell commands. This interface is available via serial port or via Telnet. Accessing the CLI via Telnet requires authentication, user name and password. The CLI input/ouput interface was construct based on the bgsh application of Robert Geer [Gee98], which allows the read of the command line and separated that in words. After this words separation, that is passed to the CLI module that was totally constructed. The CLI commands is organized on a tree structure, here each command have a father command associated (excepted the root). Each tree element can be an action (a terminal element) or a node element. With this, is possible the navigation in the commands´ tree an execute several actions. The tree organization of commands allows a easily addiction of new commands . There is defined global commands that can be executed whatever is the tree position (e.g. help command).

SNMP Alarms One of the common features that commercial WiMAX equipments have is the SNMP agent. The SNMP agent allows the remote management of the system. Since the remote management mechanism choose for this SS was based in XML files exchange via HTTP, it wasn´t implemented a SNMP agent. However, a SNMP agent can be configured to send spontaneous messages, SNMP traps, for a trigger event to a specific network place (pre-configured). This is a functionality that was pretended to WiRia SS. For that, was implement a module, SNMP Alarms, that allows the sending of SNMP traps message in any point to the system. Actually, the trap messages available are: at boot up, send the network interfaces configurations; every time that air network interface configuration change, send the new configuration. In a management interface is possible to enable/disable the sending of this messages, as so, the receiver of this messages.

System upgrade When the WiRia SS is powered up, the ARM processor (UMAC engine) runs a bootloader VxWorks image. This image, with a small size, is responsible to load the main image into the memory and then start the execute of that. The bootloader can get the main image through any supported device, for example, Ethernet or Flash. In normal operation, the main image is in the Flash memory. However, booting from Ethernet is also

possible in this SS[9]. This SS can have two main images in the Flash, which implies that two different versions of main image can be selected (via management interfaces). The main image can be upgrade through FTP or through TFTP, impling . When is proceeding to image upgrade, the current main image is maintained and the alternative image is erased. On the next boot of the SS, the upgraded image becomes the current main image.

6.3.4 Real-Time Considerations

The existence of a RTOS don´t implies the existence of the real-time system. The RTOS facilitates the creation of that, but the main point is in the correct software programming. VxWorks, as referred before, is a multitasking kernel and uses a scheduling algorithm based on fixed priorities. This can causes the blocking of a lower priority task by an higher priority task, if no time is given to lower priority to run. This must be take in count when developing tasks. On the WiRia SS, the following groups of tasks can be identified:

- *VxWorks intrinsic tasks*;
- *UMAC tasks*;
- *Network tasks*;
- *User Applications tasks.*

Is not pretended to give an extensive description of the tasks present in the WiRia SS, but to give the sensibility that UMAC tasks must have the highest priorities, because of its time requirements (MAC messages, fill the frame in correct time, ...). The network tasks must have highest priority than user applications, because, like was mention before, almost user applications depends of the VxWorks network stack, so this network services must run in high priority. In parallel to tasks, there is the interruptions, which can be see as a highest priority tasks. The interrupts service routines should execute the minimum work that only can be done here, and leave the rest of the work to tasks execution plain. In this routines, it must be avoid calling blocking functions (like input/output functions), because that can causes system blocking. In this SS, the most common interrupts are from Ethernet, timers and LMAC.

6.4 Conclusions

The Fujitsu reference kit, with the SS software package, supplies to developers a platform that have the capability to connect to a commercial Fixed WiMAX BS (Redline BS AN-100U), this with several limitations (bandwidth, frame length, ...). With this platform it is possible for developers to build its own solutions using a closed but independent UMAC module. Like was shown with the WiRia SS, several additional services can be added without the loose of UMAC performance, this if a correct programming is implemented.

[9]This only likely used when any problem have happen to VxWorks image on the Flash.

The possibility of services addition (e.g. Web server) can lead to the building of road safety services under this system. Maintaining all existing management services in WiRia SS (Web server, CLI, ...), is possible to add it a new service specially dedicated for road safety services. However, the real-time behavior of this service and the impact of that on the system must be a target of possible study. On another way, this system can be view as a transportation module of the OBU unit. As a possible transportation module, the main function of it is to receive the data from air and deliver it through Ethernet port. Like a full OBU unit or like a transportation module, is possible to transform this equipment into a road safety equipment, where the end-to-end times must be measured and verified if that achieves the requirements for road safety applications.

Chapter 7

Evaluate WiMAX equipments real-time behavior

7.1 Introduction

WiMAX features presented before shows that this wireless technology has the potential for road safety services. However, this services have special requirements, in terms of bandwidth and timeliness, that have to be accomplish by the end-to-end road safety applications, independent of the transportation technology used. In [Lin07] two types of road services are defined:

- *Critical services* - That requires an immediate response by the driver; the latency associated should be less that 100 ms;
- *Non-Critical services* - where the response of the driver is not critical for road safety improvement; the latency associated should be less that 60 s;

Those services can be matched with the potential applications referred in the chapter 1: *Safety Warning* and *Assisted Driving* as a critical services; *Traffic Management* and *Commercial applications* as a non-critical services. However, some commercial applications, like VoIP may need some real-time guarantees but they always be at lower priority than critical services. In [Lin07], is also defined that the size of critical message isn´t bigger than 1000 bytes. WiMAX, beyond guarantee the road safety services requirements, it also must leave some margin to the road safety application can process the information and alert the driver. Traffic classification (QoS) at MAC level is a WiMAX feature that allows services differentiation in terms of priority and resources used, taking in count the propose of the several service classes defined[1].

In this chapter is pretended to evaluate the behavior of available WiMAX equipments in a possible road safety environment, in order to prove the suitability of WiMAX technology for critical V2I and I2V communications. To achieve that, first, it was performed some basic functional tests (connectivity tests) and then was proceeded to a throughput analyze. After,

[1] UGS, rtPS, nrtPS, BE and additional for Mobile WiMAX ertPS.

it was assumed an hypothetical road safety messages mechanisms, in a hypothetical scenario, where was evaluate the delay for this messages, faced several traffic conditions (overload/not overload). Additional, in order to have a realistic time of the WiMAX Network Entry process, it was measured in the WiRia SS the end-to-end time of this process, in several scenarios.

7.2 Tests Specifications

For evaluate WiMAX technology for road safety communications, there were available three equipments: a WiMAX Forum certified BS, Redline AN-100U; a WiMAX Forum certified SS, Redline SU-O; and the prototype WiRia SS. This equipments follows the Fixed WiMAX specifications. Beyond the use of the WiRia SS, it was also used a commercial SS in order to compare this two SSs and thus evaluate not only WiMAX but also the WiRia SS.

The tests performed were classified on two different categories:

- **Functional Tests**: where was pretended to test some of WiRia SS´s basic functional functionality such us radio link connectivity, perform a throughput analyses in a well-known conditions (for both SSs) and verify the used of WiRia SS in a low-speed vehicle movement scenario.
- **Timing Analysis Tests**: with the intention of evaluate the sustainability of WiMAX and its QoS mechanism for road safety applications. For that, was developed an application that allows to simulate a safety messages flows, where it was tested in several data traffic conditions.

In this assessment, was defined a global scenario, represented on figure 7.1, where the BS only connects to a single SS in each time (PtP scenario). A PMP scenario wasn´t considered. Except the Radio Link and WiMAX Network Entry time measures, all others was performed on the personal computers (PCs) attached in Ethernet interface of the WiMAX equipments. Whatever the test performed, there were some parameters that was always used: the operating frequency in 3.5 GHz, a channel bandwidth of 3.5 MHz, a cycle prefix length of 1/16, a TDD scheme with a downlink and uplink sub-frames of 56% and 44%, respectively, and a frame duration of 10 ms.

7.2.1 Measure Tools

One important part in the tests executing is the measure tools used. Before starting the description of the tests, is important to refer the tools used.

Traffic Generator

For a throughput analyses and for additional data for timing analyses, it has been generated a constant data rate UDP traffic from one PC to the other. For that, it was used the MGEN tool [NCSB08], where has always been used a packet size of 512 bytes (effective data) and only the data rate was changed.

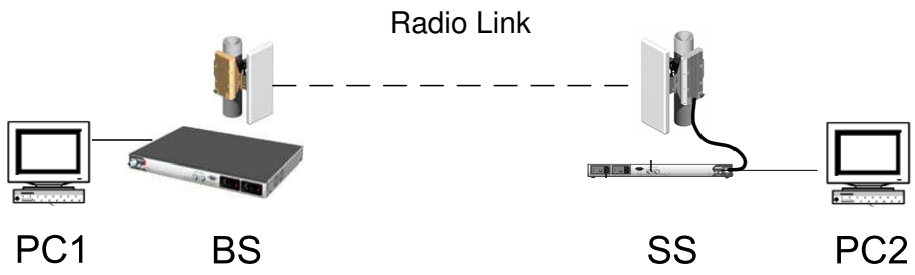

Figure 7.1: WiMAX tests global scenario

Radio Signal Parameters Acquisition

For functional tests, it was important to acquire some radio signal parameters. For this acquisition, it was development and application to remotely and automatic acquire the RF parameters measured in the WiRia SS and BS, with a specified period and a certain amount of time. For WiRia SS, using the exchange of XML files mechanism described in chapter 6, is acquired the downlink RSSI (signal strength) and carrier to interference-plus-noise ratio (CINR) (signal effectiveness). For BS, using Telnet[2], is acquired the uplink RSSI and CINR, the downlink and uplink modulation and coding and also the SS transmission power (this last one was discarded in results analysis).

Network Entry Time Measuring

For measure the WiMAX Network Entry time of the WiRia SS, was build an internal SS mechanism which allow the detection of the start and the end of the this process, measuring the time between that. It is important to refer that, with this application, is not possible to measure the different phases of the Network Entry process, mention on chapter 4. This applications runs in a low priority task on WiRia SS and polls the UMAC state for detect the beginning and the ending of process.

Safety Messages Mechanism

In order to evaluate the WiMAX technology and its QoS services for road safety applications, was development a mechanism that simulate the sending of safety messages. This mechanism consists in sending a message from one PC to the other where the message is sending back to the origin PC. This allows the measure of the correct delay for the total path travelled by this message (round trip time (RTT)). This process can be repeated for several messages. It was consider a 200 ms timeout (double of 100 ms defined above for maximum delay for critical messages) for receive the message in origin PC. If that happens, the message

[2]Here, it was used a tool for automating interactive applications such as Telnet and FTP, the Expect tool [oST08]

is considered lost. The size of the message used is 1000 bytes. Using this message mechanism with additional traffic will permit the analyses of suitability WiMAX for critical road services.

7.2.2 Functional Tests

Radio Link connectivity

The main objective of the radio link connectivity tests was to verify the correct operation of WiRia SS when connected to the BS. For this, it was measure in both downlink and uplink directions the signal strength (RSSI), the signal effectiveness (CINR) and the modulation and coding used. It was made this measures in several points where the BS is fixed at one point and the WiRia SS was placed in several points with different distances to the BS, but always with optical LOS. It was also made a simple throughput analysis in order to test the end-to-end connectivity between the two PCs. This throughput analyse consisted in generating 1Mbps of UDP data from one PC to another where was measured the receiving rate. This was also executed in other way (bidirectional traffic, 2Mbps at both ways). In some of that points, was preformed this same tests but generating 10Mbps in each way. Additional, in each point as measure the WiMAX Network Entry time.

For this tests, was used of two different antennas: an omnidirectional antenna developed at the Institute of Telecommunications; and a commercial antenna, from Redline Communications, with 15º directionality and with 18 dBi gain. Preferentially, was used the omnidirectional antenna, but there were some points where wasn´t possible to have link connection with this antenna, so the directional antenna was used.

Low speed connectivity

In a scenario where the BS and the SS are at a fixed location, the radio link conditions will not have constantly sudden variations[3]. In another way, if an SS is in movement, the radio link conditions can change quickly and the system may not be able to adjust its radio parameters in order to stay connected. Here, the PHY and radio parts of the fixed or mobile WiMAX can lead to different significant results. The intention of this test was to evaluate the behavior of the WiRia SS in a movement scenario, where the BS was in a fixed point and the SS was in movement, achieving a maximum speed of 30 km. In figure 7.2 is represented the place here this tests were performed. Two different situations had been tested:

- The SS is stopped and after execute registering to a BS starts to move;
- The SS enters in the BS coverage area already in movement and has to perform the registration process while moving.

For both situations, was checked the network entry time. In this test was measure, during movement, the RSSI and CINR in downlink and it was also verified if end-to-end connection

[3]In this scenario, conditions can changes due factors like weather or the appearance of a temporary obstacle.

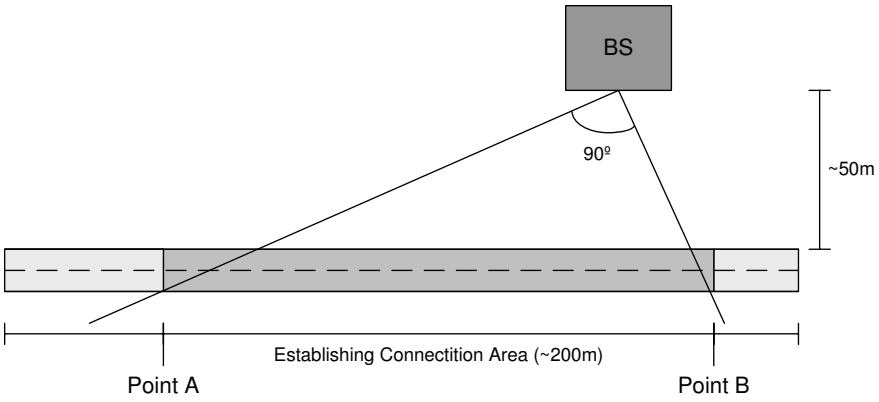

Figure 7.2: Low speed test scenario

is maintained (check connection between the two PCs by executing the ping command[4]). The antenna used on WiRia SS was the omnidirectional antenna.

Throughput analyses

The final functional test performed was a throughput analysis, where was pretended to verify the maximum throughput allowed by WiRia SS. This test also performed with the Redline SS, in the same conditions, in order to compare results. The radio propagation conditions used can be considered ideal, because the distance between BS and SS was less than 10 m. It was created two service flows, one in downlink other in uplink, with the rtPS service class. Then, simultaneous in both PCs was generated data at 256 kbps during two minutes, be this transmitted over the air to the opposite PC. This was repeated to several data rates: 512, 1024, 2048, 4096, 6144 and 8192 kbps. This test with several data rates was also repeated for a different service class in the flows (BE service class).

7.2.3 Timing Analysis Tests

The main objective of timing analysis tests is to assess WiMAX for critical road safety applications. Using the safety messages mechanism developed and described above, is possible to measure the RTT of several messages and evaluate the performance of WiMAX equipments for some traffic data rates conditions (even in traffic overloaded).

The Redline BS supports only two service classes: BE and rtPS. Between this two classes, rtPS offers more real-time guarantees, so, for a road safety scenario, this class would be used for critical services. However, in this work, it wasn´t only was used the rtPS class for safety messages, but also the BE class. So, this tests can be divided in parts: one part where was used the safety messages in a rtPS service and other traffic in a BE service; another part

[4]Ping is computer network tool used by Internet Control Message Protocol (ICMP) to test connectivity between machines across an IP network

Point	Distance to BS (m)	DL CINR (dB)	DL RSSI (dBm)	UL CINR (dB)	UL RSSI (dBm)	SS antenna used	Network Entry (s)
1	31	26.0	-47.1	28.0	-68.0	Omnidirectional	2.85
2	71	25.5	-50.3	28.0	-67.2	Omnidirectional	2.24
3	78	26.2	-46.2	27.7	-68.5	Omnidirectional	2.04
4	98	24.3	-51.4	28.2	-67.3	Omnidirectional	2.24
5	140	24.1	-65.0	27.8	-67.6	Omnidirectional	2.38
6	200	25.5	-56.2	27.6	-68.3	15º Directional	2.28
7	240	25.2	-53.2	27.9	-67.2	15º Directional	2.85
8	330	24.0	-58.1	26.9	-66.1	15º Directional	2.38

Table 7.1: Radio Link connectivity results

where was used the safety messages in a BE service and other traffic in a rtPS service. This tests was performed for both WiRia SS and Redline SS.

Independent of the configuration used (messages in rtPS or messages in BE), it was created four service flows: two for rtPS; and two for BE. The round trip time of the messages was measured for several traffic data rates (in the opposite service class and in both downlink and uplink): 0, 512 1024, 2048, 4096 and 8192 kbps.

7.3 Tests Results

This section presents the results obtained from the tests described above. The tests organization is the same that as used in specification.

7.3.1 Functional Tests

Radio Link connectivity

The radio link connectivity test, as described before, have the objective to validate the correct operation of WiRia SS, by measuring several radio link parameters in some points with different distances to BS. In table 7.1 is presented the radio parameters measured in the considered points, as so, the type of antenna used and the WiMAX Network Entry time for each point. The downlink and uplink modulation and coding used in each point is not represented in this table because always when connectivity was established, the modulation was 64QAM and the coding was 3/4, the maximum supported by the equipments.

Using the omnidirectional antenna, was possible to have connectivity until 140 m, as show in table 7.1. Since this distance, the directional antenna was used in order to get connectivity to BS. However, independently of antenna used, is possible to say that the radio signal quality was good for all points since the CINR (signal effectiveness) is always upper than 24.0 dBm[5]. But is possible to see that the signal strength (RSSI) falloff is function of the distance, which can cause the appearance of some connections problems, such as noise power increase.

[5]The threshold defined in the Redline BS for change to highest modulation and coding is 23.25 dBm for CINR

Point	Throughput			
	1 Mbps for DL (kbps)	10 Mbps for DL (kbps)	1 Mbps for UL (kbps)	10 Mbps for UL (kbps)
1	849.30	-	991.65	-
2	991.26	5509.79	991.26	3855.42
3	855.60	-	991.23	-
4	991.23	-	990.68	-
5	854.68	-	971.80	-
6	863.41	5628.73	990.56	3682.12
7	991.44	-	991.85	-
8	852.15	5493.66	991.12	3602.94

Table 7.2: End-to-End connectivity (throughput obtained)

For the points presented in the table 7.1, it was also performed the end-to-end connectivity test which consist on the sending 1 Mbps of data in the downlink and other 1 Mbps to the uplink, and verify the received rate. For points 2, 6 and 8, it was also performed this test but with 10 Mbps instead of the 1 Mbps. The results obtained are in table 7.2.

In presence of the results in table 7.2, the throughput obtained when 1 Mbps is generated is similar to the expected one, but with better results in the uplink than in downlink (more losses occurred in this last direction). When is generated 10 Mbps, is expected that the data-rate received is lower because of the channel limitation[6]. For this, the downlink data rate obtained was approximately 5.5 Mbps and the uplink approximately 3.7 Mbps, which case a downlink/uplink relationship of 59.8%, instead of the 56 % defined on the BS for this tests. This could be happen because of the losses either on the uplink or either on SS internal packet processing for this overloaded situation.

Low speed connectivity

As referred in tests specification, the low speed tests objective is to verify the behavior of WiRia SS in a movement scenario, which, for this case, was considered the scenario represented in figure 7.2. For the situation where the SS is stopped, execute the Network Entry process and then starts to move from 0 Km to 30 Km (slowly), it is possible to say the results were satisfactory because was possible to maintain the end-to-end connectivity between the points A and B, which are the border points where is possible to have establishment of connection between BS and SS, whatever the direction (A to B or B to A). However, for the situation where the SS enter to the *establish connection area* already at 30 km, the results was not so good. In the direction point A to point B was possible to establish connection and maintain the end-to-end connectivity, but in the direction B to A the establishment of connection was not possible. Observing the figure 7.2, is possible to view that the distance from point A to BS is bigger than the distance from point B to BS, so, moving SS from A to B implies the distance decrease from SS to BS, occurring the opposite when moving from B to A. This can justify the results obtained because the signal adjust is difficult if SS and BS get more distant.

To show the signal variation during the movement, in figure 7.3 is represented the RSSI

[6]Is not possible to have a throughput of 10 Mbps in one direction using the same radio link parameters used for this tests.

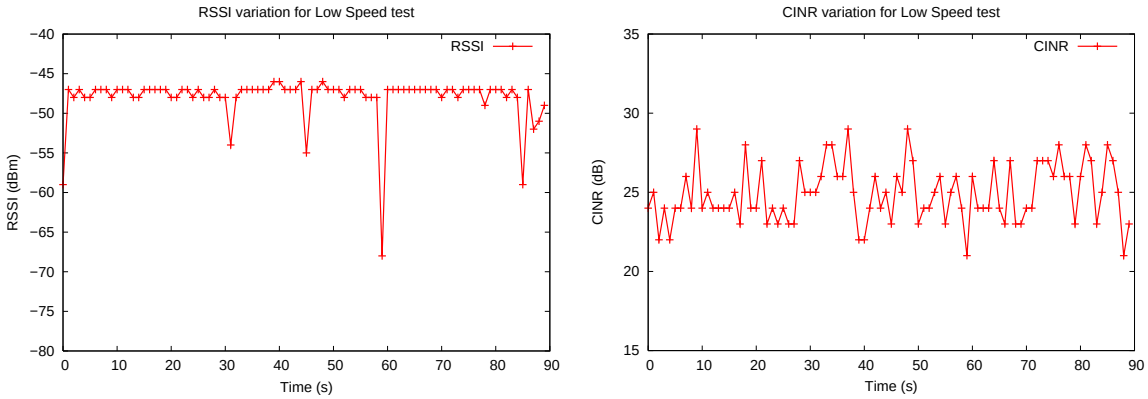

Figure 7.3: Low speed connectivity signal variation in downlink

---

and the CINR variation for the situation where the SS moves from point A to B after execute the registration process. Analyzing this figure, is possible to view the sudden variations that happens on the RSSI and the inconstant CINR value. Although the sudden signal variations (for -48 to -70 dBm), it was always possible to decode the signal. One way to avoid this sudden variations, and also improve the stability of the radio link, is use multiple antennas techniques [JGA06].

Additional, for this movement tests was also measure the Network Entry time. When the connectivity was possible, the value obtain stays between 2 and 3 s, independent of the situation (A to B or B to A; stopped or moving). The mean value for all values registered is 2.48 s.

Throughput analysis

This test, as mention in specifications, has the objective to evaluate the throughput of the WiRia SS. To compare results, it was also performed for Redline SS. In figure 7.4 is represented the results obtained in the receiver for the several data-rates generated and for each service class used (BE and rtPS).

It is possible to say that the behavior for both SSs is similar for data-rates lower or equal than 4 Mbps, where the downlink and uplink data-rates received are similar to data-rates transmitted (for both service classes: BE and rtPS). For data-rates higher the 4 Mbps it is possible to see that the Redline SS have a bigger uplink rate than the WiRia SS, for both service classes. Like has mention before, this may be due to losses either on the uplink transmission or either on WiRia SS internal packet processing on an overloaded situation. This can also explain the significatively lower received data-rate for 6 Mbps and 8 Mbps than data-rate received for 4 Mbps (from 3.9 Mbps to 3.6 Mbps), this for WiRia SS and for rtPS service class. For the downlink, the behavior of both SSs for all data-rates is similar, and the received rate is similar to the expected one.

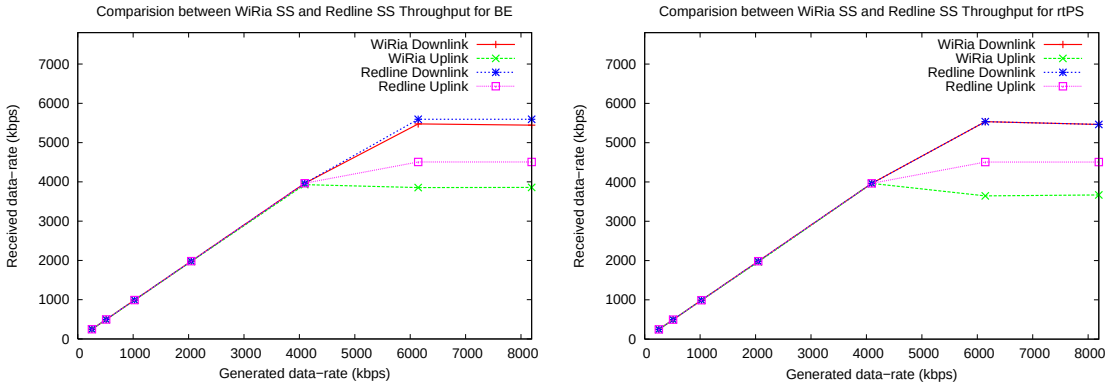

Figure 7.4: Throughput comparison between WiRia SS and Redline SS (BE and rtPS)

BE Data Rate (kbps)	Maximum rtPS Delay (s)	Minimum rtPS Delay (s)	Average rtPS Delay (s)	rtPS Standard Deviation (s)	rtPS Jitter (s)
0	0.04541	0.01944	0.03019	0.00310	0.02598
512	0.04543	0.01508	0.03110	0.00409	0.03034
1024	0.05100	0.01379	0.03082	0.00423	0.03721
2048	0.05265	0.01394	0.03161	0.00503	0.03871
4096	0.08244	0.02874	0.04510	0.00669	0.05371

Table 7.3: rtPS Delay using the WiRia SS

7.3.2 Timing Analysis Tests

WiRia SS

First, it was performed the safety messages simulation tests using the WiRia SS. In table 7.3 is represented the results obtained when the rtPS was used for safety messages and BE was used for data traffic. The results when was used the BE for safety messages and rtPS for data traffic is represented in table 7.4. It was measure the mean, the maximum and the minimum RTT, also referred as delay in this work, and it was calculated the delay standard deviation (which indicates the samples deviation from the mean delay) and the jitter (which indicates the difference between the maximum and minimum delay[7]). It is important to refer that, for this SS, when the was generated 8192 kbps of data for each way, for both situations (messages on rtPS or messages on BE), it was occurred message timeout for all messages sent, so the missing of this value on tables.

Comparing the values of table 7.3 (rtPS for messages) and table 7.4 (BE for messages) is possible to say that the rtPS, like was expected, shows some real-time guarantee in presence of other low priority traffic. For values lower than 2048 kbps of additional data, the behavior for both situations is similar, and match the needs for critical services (maximum delay obtain 70 ms for all cases in this situation). However, when the data traffic becomes higher, it can be noticed some differences between the two classes. For 4096 kbps data-rate, the delay for

[7]Jitter definition in this work

rtPS Data Rate (kbps)	Maximum BE Delay (s)	Minimum BE Delay (s)	Average BE Delay (s)	BE Standard Deviation (s)	BE Jitter (s)
0	0.04397	0.01490	0.02816	0.00485	0.02907
512	0.05198	0.01627	0.02580	0.00689	0.03571
1024	0.07235	0.01554	0.02672	0.00844	0.05681
2048	0.07009	0.01636	0.03225	0.01247	0.05372
4096	0.20000	0.03331	0.12941	0.05213	0.16669

Table 7.4: BE Delay using the WiRia SS

	Maximum rtPS Delay (s)	Minimum rtPS Delay (s)	Average rtPS Delay (s)	rtPS Standard Deviation (s)	rtPS Jitter (s)
rtPS DL	0.060153	0.022669	0.04018264	0.00482401	0.037484
rtPS UL	0.052009	0.015312	0.03144916	0.00435835	0.036697

Table 7.5: rtPS Delay with 8192 kbps BE traffic (Downlink and Uplink separately)

messages for BE scenario grows getting a mean value of 129 ms and for some messages the timeout was occurred. For rtPS messages scenario it was noticed an increase of the delay, in comparison of values with for lower data-rates.

In the BE scenario, independently of the SS used, the messages are forward through the air in service flows with low priority than the service flows for the generated data. The low priority is implicit on the class of service used: is not possible to have a BE service flow with higher priority than a rtPS service flow. Due this, for data-rates bigger than the maximum throughput, the messages will be discarded and timeout occurs.

On the other hand, for the rtPS scenario, the messages travels through higher priority services flows so, it should have more priority than the generated data and should not be discard and also the real-time guarantees should be maintain. But this not happen for the WiRia SS. For this scenario, it was verified that when the data-rate generate is 8192 kbps (for each way) for all messages sent a timeout was occurred. This could happen because of the WiRia SS behavior in traffic overload conditions. However, to best evaluate the real-time guarantees for rtPS, it was performed an additional test where it was only generated traffic in on way (downlink or uplink), where the values obtained is represented in table 7.5. For this situation is possible to verify that the requirements for critical services are accomplished.

Final discussion In the presence of the results above for WiRia SS, it could be see when is used the rtPS class for messages flow is possible to have real-time guarantees in order to supply a road safety critical service, but only when don´t occur traffic overloaded situation. The end-to-end delay obtained (mean value) when rtPS service class was used for safety messages and generate data-rates lower or equal 4096 kbps, is lower than the value that is defined for maximum delay for a critical service (100 ms), where the maximum delay obtained is also lower than this defined value. The problem demonstrated by WiRia SS in traffic overload conditions could a target of a future study.

BE Data Rate (kbps)	Maximum rtPS Delay (s)	Minimum rtPS Delay (s)	Average rtPS Delay (s)	rtPS Standard Deviation (s)	rtPS Jitter (s)
0	0.05197	0.01996	0.03428	0.00642	0.03201
512	0.04794	0.01586	0.02956	0.00557	0.03208
1024	0.04524	0.01523	0.02955	0.00605	0.03001
2048	0.04852	0.01590	0.02878	0.00579	0.03261
4096	0.05609	0.02421	0.03949	0.00647	0.03188
8192	0.06390	0.02963	0.04606	0.00651	0.03427

Table 7.6: rtPS Delay using the Redline SS

rtPS Data Rate (kbps)	Maximum rtPS Delay (s)	Minimum rtPS Delay (s)	Average rtPS Delay (s)	rtPS Standard Deviation (s)	rtPS Jitter (s)
0	0.04561	0.02453	0.03175	0.00376	0.02108
512	0.05940	0.02564	0.03286	0.00410	0.03376
1024	0.06396	0.02833	0.04281	0.00455	0.03563
2048	0.05594	0.02777	0.04269	0.00425	0.02817
4096	0.06037	0.02794	0.04359	0.00481	0.03243

Table 7.7: BE Delay using the Redline SS

Redline SS

The tests performed for WiRia SS, presented above, were repeated for the Redline SS. The messages in rtPS class test results is in table 7.6 and the messages in BE class test results is in table 7.7. In this last case, the values for 8192 kbps where not presented because timeout was occurred for all messages, for the reason explain above for the timeout in BE service flows in the presence of rtPS service occupying all available bandwidth.

For data-rates lower or equal than 4096 kbps, the behavior for the two test situations (rtPS or BE service flows for messages), don´t present any significantly difference and the delay values for critical services are accomplished (maximum delay of 60ms). However, when messages travels on the rtPS flows the delay values for the different data-rates tested is more constant than the delay values for messages in BE flows. For 8192 kbps data-rate, in opposite of what happens for WiRia SS, the real-time guarantees for rtPS flows are supplied, offering a end-to-end delay in lower than the delay defined for critical services.

Final discussion Using Redline SS with the rtPS class for messages flows is possible to provide road safety critical services because, despite of traffic overload on the BE service flows. The rtPS delay, standard deviation and jitter do not increase and fulfilling the safety services delay requirements. However, for situations when the data-rate of non-safety traffic is lower or than than 4096 kbps, supply road safety services through BE flows is also possible.

Compare WiRia SS and Redline SS

After described the tests results for each SS individually, is possible to compare the performance of both SSs in simultaneous. In figure 7.5 is presented a comparison of mean, maximum

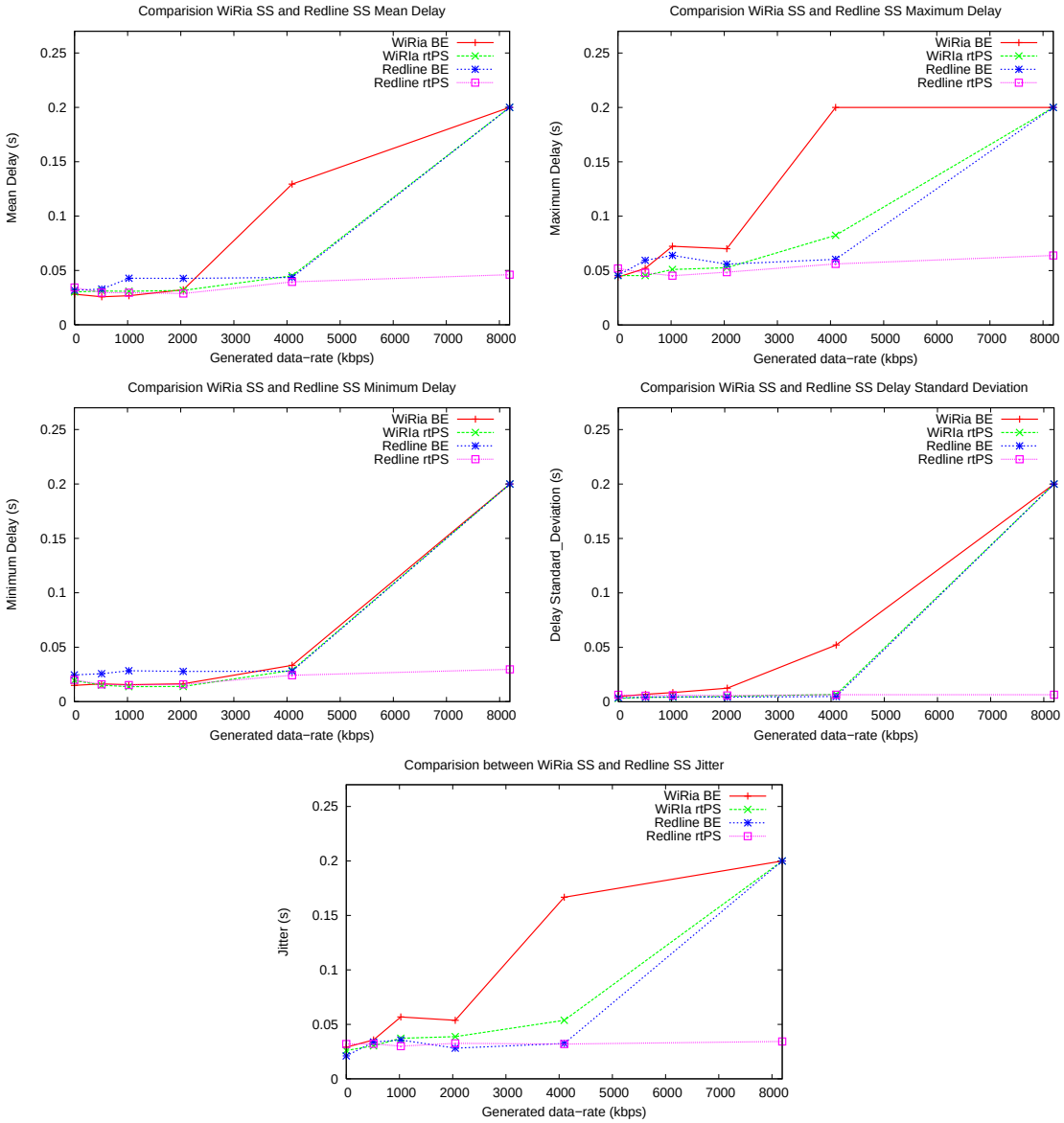

Figure 7.5: Timing Analysis Comparison between WiRia SS and Redline SS

and minimum delay, the jitter and the standard deviation in simultaneous for WiRia SS and for Redline SS[8].

Observing the figure 7.5, it is possible to see the major drawback of WiRia SS: in a traffic overload situation and for rtPS message flows the real-time guarantees aren´t supplied. This drawback doesn´t happen for Redline SS. It is also possible to view the better behavior of Redline SS in terms of jitter. However, both SSs can provide critical services using rtPS service class to accomplish real-time agreements of that independently of the BE traffic (expect an

[8]For 8192 kbps data-rate, it was considered the maximum value possible, 200 ms, when time-out was occurred for all messages

overload situation for WiRia SS). So, it is possible to have simultaneous critical and non-critical services using the WiMAX equipments.

7.4 Conclusions

This chapter has introduced the definition of road safety critical and non-critical services, as so, the maximum latency for these services (less than 100 ms for critical; less than 60 s for non-critical) and the critical service messages size (1000 bytes), as defined in [Lin07]. It was also matched this services to potential applications defined in chapter 1, where Safety Warning and Assisted Driving applications as critical services and Traffic Management and Commercial Applications as non-critical service.

The functional tests presented above had shown the correct operationally of WiRia SS, which was build with Fujitsu Reference Kit as base. However, the mobility tests executed show that WiRia SS, as representant of Fixed WiMAX equipments, is not good for this type of scenario, where the sudden signal variations are constants. It is very probably that Mobile WiMAX have better results for this, but additional techniques must be considered, such as multi-antennas. In terms of throughput, both SSs (WiRia and Redline) presented a similar behavior, where Redline SS presented with best uplink behavior (4.4 Mbps instead of 3.9 Mbps of WiRia SS).

Using the equipments available, which have Fixed WiMAX features, it was possible to evaluate WiMAX for critical services in terms of traffic differentiation and real-time guarantees. The timing analysis tests show that WiMAX rtPS service class is adequate to provided critical services, even in a traffic overloaded situation for low priority flows (just for Redline SS). WiRia SS presents a drawback for traffic overload situation, which can be a point of improvement for this SS. However, WiRia SS shows that is able to satisfy the critical services demands when is not in a overload situation.

Finally, the Network Entry time obtained for WiRia SS, independent of the of the situation where was performed (fixed or movement), stays between 2 and 3 s. This value is 3 or 4 times bigger than the value calculated in chapter 4 for an hypothetic situation. However is not possible to identify in which step the Network entry Time process takes more or less time than the assumed. Assuming the same velocity considered in chapter 4 for Network Entry analysis for vehicular communications (250 km/h), the WiRia SS travels 208 m before get connected.

Chapter 8

Conclusions

8.1 Final Conclusions

Road safety is a serious concern that gets the attention of governmental entities all over the world. A serious effort has been done to reduce road accidents, as shown in the several European initiatives presented in the chapter 2. Here, different approaches have been considered to improve road safety, where most depend on the ability of the vehicles to communicate with each other (V2V) or with RSU (V2I), and where the basis are the wireless communications. Several wireless technologies have been considered for vehicular communications, e.g. standards (like GSM) or improved standards (like DSRC). In chapter 2 it is also shown that WiMAX technology can be considered for vehicular communication, due to the several usage examples, such as a video conference at 45 miles/h or HDTV reception at 140 km.

Assessing WiMAX for V2I and I2V communications was the main objective of this work. Some aspects of this technology were presented in chapter 3, where technical details and some salient features were discussed, such as QoS support, which shows the potential of this technology for V2I communications. Supported on the WiRia project, it was possible to have access to Fixed WiMAX commercial equipments and a prototype SS, WiRia SS, in order to evaluate WiMAX sustainability. In chapter 6 it is shown the effort that had be done to transform a development board into an operation SS. There, it was possible to add the management services and to correct some internal packet forwarding mechanisms. However, due to the use of a closed UMAC module, it was not possible to add or modify any WiMAX MAC feature.

Functional tests performed using the WiRia SS showed a very satisfactory behavior, in terms of connectivity at a fixed point and maximum throughput. However, for a movement scenario, this SS appears as inadequate due to the occurrence of sudden variations on the received signal strength (RSSI), the inconstant value of signal effectiveness (CINR) and the failures in the connection establishment verified when the SS is already in movement. Using techniques based in multiple antennas, such as multiple-input, multiple-output (MIMO) antennas, it is possible to improve the signal reception and transmission. Also, using other PHY, such as OFDMA (used in Mobile WiMAX), the results could be improved.

Road safety application, described in chapter 1, can be classified as critical (*Safety Warn-*

ing and *Assisted Driving*) and non-critical (*Traffic Management* and *Commercial application*) services. The requirements define for critical services were less than 100 ms of latency and 1000 bytes of message size. Using WiMAX rtPS service class, it is possible to satisfy this critical service requirements, and thus supply road safety services. It was also proved that it is possible to obtain a coexistence of both critical and non-critical services, maintaining critical services demands. However, WiRia SS presents a problem under traffic overloaded situations, which must be considered for a future use of this SS under these circumstances.

Finally, the study of the Network Entry process (chapter 4) shows that the time required to execute this should be taken into account when projecting a road safety system. The values obtained for the WiRia SS (lower than 3 s) show that, with the WiRia SS traveling at 250 km/h, 208 m are needed before it gets connected to the BS.

8.2 Future Work

This dissertation introduces the great potential of WiMAX for road safety vehicular communications, mainly in terms of the real-time guarantees for critical services. However, more work has to be done to validate this wireless technology for road safety scenarios. It must also be taken into account the proposal of small changes to this wireless technology in order to improve the efficiency for this type of scenarios.

Nowadays, V2I and I2V communications must be performed at high-speed and so the appearance of some radio propagation effects has to be considered, such us Doppler Effect (mention in chapter 4), specially if high signal bandwidth is used. This must be a point of major importance in the study of a vehicular communication system because the radio propagation is the basis of wireless communications. Here, the use of Mobile WiMAX equipments can be advantageous, as shown in some initiatives presented in chapter 2, due to some additional features in PHY and MAC. However, it is also possible to continue exploring Fixed WiMAX for V2I and I2V communications, being the equipment simplicity (and thus the cost) its major advantage.

Another important concern is the existence of multiple vehicles in a single RSU area, and so leading us to the presence of a PMP scenario. A possible target of a future study is to evaluate the real-time guarantees under this scenario. Here, also the network entry process could be studied, now in a multiple collisions environment, which can have a great impact on the time to perform that. It is also possible to consider a real test scenario, where some vehicles, each one with its OBU equipment, connect to a single RSU.

In the OBU development perspective, it is also possible to indicate some aspects to improve its evolution. As shown in the chapter 6, it is possible to have network services communicating through the air. Exploring a road safety service as an additional network service, IP based, could be an advantage in the sense that it would enable a faster and more scalable services appearance. This also allows to increase the simplicity in the implementation of multiple services under the same equipment. However, dedicated applications can be considered (not IP based), in order to reduce complexity of the system or to fulfill some extremely time critical requirements.

Bibliography

[20008] Smartway 2007. Smartway 2007 demo, trial operation on metropolitan expressway and spread of smartway project, April, 2008. http://www.its.go.jp/ITS/index/indexSW2007.html.

[Alv07] Alvarion. Alvarion, July, 2007. http://www.alvarion.com/.

[Ame06a] Fujitsu Microelectronics America. Mb87m3550, the fujitsu wimax 802.16-2004 soc. June, 2006. http://us.fujitsu.com/micro.

[Ame06b] Fujitsu Microelectronics America. Wimax soc reference design. November, 2006. http://us.fujitsu.com/micro.

[Ame07] Fujitsu Microelectronics America. Mb87m3550 wimax soc reference design kit, September, 2007. http://www.fujitsu.com/us/services/edevices/microelectronics/broadbandwireless/products/#fixed.

[AU08] APCA and UTAD. 8th portuguese conference on automatic control - controlo 2008, April, 2008. http://home.utad.pt/controlo2008/.

[BRI08] BRISA. Brisa - auto-estradas de portugal s. a, April, 2008. http://www.ua.pt/.

[CE06] Subbu Ponnuswamy Carl Eklund, Roger B. Marks. *WirelessMAN, Inside the IEEE 802.16TM Standard for Wireless Metropolitan Networks*. Standards Information Network IEEE Press, 2006.

[Com07a] Redline Communications. Redline communications, July, 2007. http://www.redlinecommunications.com/.

[Com07b] Sequans Communications. Sequans communications - fixed wimax, September, 2007. http://www.sequans.com/products/fixed_wimax.php.

[COM08a] COM2REACT. Com2react, January, 2008. http://www.com2react-project.org/.

[COM08b] COM2REACT. Com2react fact sheet, January, 2008. http://ec.europa.eu/information_society/activities/esafety/doc/rtd_projects/fact_sheets/call_4/com2react.pdf.

[COM08c] COMeSafety. Comesafety, January, 2008. http://www.comesafety.org/.

[COO08] COOPERS. Coopers, January, 2008. http://www.coopers-ip.eu/.

[CVI08a] CVIS. Cvis, January, 2008. http://www.cvisproject.org/.

[CVI08b] CVIS. Cvis high level architecture, January, 2008. http://www.cvisproject.org/.

[daI07] Ministério da administração Interna. Sinistralidade rodoviária 2006, elementos estatísticos., March, 2007. http://www.mai.gov.pt/.

[eF08] eSafety Forum. esafety forum, January, 2008. http://ec.europa.eu/information_society/activities/esafety/index_en.htm.

[eSa08] eSafety. esafety, January, 2008. http://ec.europa.eu/information_society/activities/esafety/index_en.htm.

[ETS08] ETSI. Dedicated short-range communications (dsrc), April, 2008. http://www.etsi.org/WebSite/Technologies/DSRC.aspx.

[Eur07] Fujitsu Microelectronics Europe. Wimaxtm 802.16-2004 soc, mb87m3400 fact-sheet. October, 2007. http://emea.fujitsu.com/microelectronics.

[For08] WiMAX Forum. Wimax forum, January, 2008. http://www.wimaxforum.org.

[Gee98] Robert Geer. Bgsh: A vxworks shell with command line editing, December, 1998. http://www.xmission.com/ bgeer/bgsh.html.

[Gro08] Computer Support Group. Vehicle stopping distance and time, March, 2008. http://www.csgnetwork.com/stopdistinfo.html.

[Har05] A. Hart. The development of v2v & v2i communications in europe. January, 2005. SBD.

[IEE04] IEEE. *Standard 802.16-2004. Air interface for fixed broadband wireless access systems*, 2004.

[IEE05a] IEEE. *Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment 1: Management Information Base*, 2005.

[IEE05b] IEEE. *Standard 802.16e-2005. Part16: Air interface for fixed and mobile broadband wireless access systems-Amendment for physical and medium access control layers for combined fixed and mobile operation in licensed band*, 2005.

[IEE08] IEEE. The ieee 802.16 working group on broadband wireless access standards, January, 2008. http://www.ieee802.org/16/.

[IET83] IETF. *RFC 868 - Time Protocol*, 1983.

[IET97] IETF. *RFC 2131 - Dynamic Host Configuration Protocol*, 1997.

[Inc08] Alpine Electronics Inc. Alpine, April, 2008. http://www.alpine.com/.

[Ini08] Intelligent Car Initiative. Intelligent car initiative, January, 2008. http://ec.europa.eu/information_society/activities/intelligentcar/index_en.htm.

[Int07] Intel. Intel wimax technology, September, 2007. http://www.intel.com/technology/wimax/index.htm.

[INT08] INTEL. Intel^R, April, 2008. http://www.intel.com/.

[JGA06] Rias Muhamed Jeffrey G. Andrews, Arunabha Ghosh. *Fundamentals of WiMAX*. Prentice Hall, 2006.

[Kar06] Frank Kargl. Vehicular communications and vanets. September, 2006. ULM University.

[Lin07] Dr.J.H. Linssen. Coopers - gprs and v2i communication, June, 2007. Aalborg ITS.

[Ltd08] Runcom Technologies Ltd. Runcom, April, 2008. http://www.runcom.com/.

[NCSB08] Networks and Naval Research Lab Communication System Branch. Multi-generator (mgen), April, 2008. http://cs.itd.nrl.navy.mil/work/mgen/.

[Net07a] Airspan Networks. Airspan networks, July, 2007. http://www.airspan.com/.

[Net07b] Aperto Networks. Aperto networks, July, 2007. http://www.apertonet.com/.

[Nua07] Louftani Nuaymi. *WiMAX technology for broadband wireless access*. John Wiley & Sons, Ltd, 2007.

[oA08] University of Aveiro. University of aveiro, April, 2008. http://www.ua.pt/.

[OEI08] Ltd. OKI Electric Industry, Co. Oki, April, 2008. http://www.oki.com/en/.

[oST08] National Institute of Standards and Technology. The expect home page, April, 2008. http://expect.nist.gov/.

[oT08a] Institute of Telecommunication. Institute of telecommunication in aveiro, April, 2008. http://www.it.pt/.

[oT08b] U.S. Department of Transportation's. Research and innovative technology administration, April, 2008. http://www.rita.dot.gov/.

[Pap08a] WiMAX Forum White Paper. Mobile wimax-part i: A technical overview and performance evaluation, January, 2008. http://www.wimaxforum.org.

[Pap08b] WiMAX Forum White Paper. The wimax forum certified^{TM} program for fixed wimax^{TM}, January, 2008. http://www.wimaxforum.org.

[PB07] Evangelos Kranakis Paul Boone, Michel Barbeau. Strategies for fast scanning and handovers in wimax/802.16. May, 2007. School of Computer Science, Carleton University.

[Pla08] NEM European Technology Platform. Mobile wimax 16e field trials, October, 2008. http://www.nem-summit.eu/.

[Pro08a] Seventh Research Framework Program. Seventh research framework program, March, 2008. http://cordis.europa.eu/fp7/home_en.html.

[Pro08b] Sixth Framework Program. Sixth framework program, January, 2008. http://cordis.europa.eu/fp6/fp6_glance.htm.

[Pro08c] SUIT Project. Suit - scalable, ultra-fast and interoperable interactive television, April, 2008. http://suit.av.it.pt/.

[PTI08] SA Portugal Telecom Inovação. Pt inovação, April, 2008. http://www.ptinovacao.pt/.

[Riv03] Wind River. Vxworks network programmer´s guide, April, 2003. http://www.windriver.com/.

[Riv07] Wind River. Wind river, September, 2007. http://www.windriver.com/.

[RR06] Nada Golmie Richard Rouil. Adaptive channel scanning for ieee 802.16e. October, 2006. National Institute of Standards and Technology.

[SAF08] SAFESPOT. Safespot, January, 2008. http://www.safespot-eu.org/.

[Sem07] Aspex Semiconductor. Aspex wimax development kit, September, 2007. http://www.aspex-semi.com/pages/products/products_tools_wimaxkit.shtml.

[Sem08] SiGe Semiconductor. Sige semiconductor wimax products, April, 2008. http://www.sige.com/index.php/products/details/category/wimax.

[Sho08] Consumer Electronics Show. 2008 international ces, April, 2008. http://www.cesweb.org/.

[Sof07] GoAhead Software. Web server, September, 2007. http://www.goahead.com/products/webserver/Default.aspx.

[Sys08] Intelligent Transport System. Cooperative intersection collision avoidance systems, April, 2008. http://www.its.dot.gov/cicas/.

[TEL08] TELESAL. Telesal, rede de competências em telecomunicações e tecnologias de informação, April, 2008. http://www.telesal.pt/.

[Wav07] Wavesat. Wavesat - evolutive wimax series, September, 2007. http://www.wavesat.com/products/evolutive.html.

[Wir07] Telecis Wireless. Telecis wireless - products overview, September, 2007. http://www.telecis.com/.

[Zee07] Ali Zeeshan. Build wimax base stations, subscriber stations. June, 2007. Fujitsu Microelectronics America.