André Amaral Costa

AVALIAÇÃO DE UM SISTEMA WIMAX PARA APLICAÇÕES VEÍCULO-INFRAESTRUTURA

André Amaral Costa

AVALIAÇÃO DE UM SISTEMA WIMAX PARA APLICAÇÕES VEÍCULO-INFRAESTRUTURA

ASSESSING WIMAX FOR VEHICULAR COMMUNICATIONS APPLICATIONS

Dissertation presented to the University of Aveiro to fulfill the necessary requirements for obtaining a Master Degree in Electronic and Telecommunications Engineering, written with the scientific orientation of Prof. Paulo Pedreiras, Professor at the Electronic, Telecommunications and Informatics Department at University of Aveiro.

Júri

Presidente

Dr. António Manuel de Brito Ferrari Almeida
Professor Catedrático da Universidade de Aveiro

Vogais

Dr. José Alberto Gouveia Fonseca (Co - Orientador)
Professor Associado da Universidade de Aveiro

Dr. Francisco Manuel Madureira e Castro Vasques de Carvalho
Professor Associado do Departamento de Engenharia Mecânica e Gestão Industrial da Faculdade de Engenharia da Universidade do Porto

Prof. Dr. Paulo Bacelar Reis Pedreiras (Orientador)
Professor Auxiliar Convidado da Universidade de Aveiro

Acknowledgements

First of all, I would like to express my gratitude to my supervisor and co-supervisor, Prof. Paulo Pedreiras and Prof. José Alberto Fonseca, for their guidance and help during this past year that made possible to perform my study.

I would also like to thank my project colleague, Hugo, because without the work that we performed together and help that we gave to each other, this study wouldn't be possible to achieve.

I would also like to show my gratitude to Eng. Álvaro Gomes from PT Inovação because he was always ready to help. Thank you also to my other project colleague, Miguel Pereira, that was always supportive.

I would like to thank to the person who helped me the most during this past year. So, I would like to thank my girlfriend, Filipa, for being there, helping me in this past three years and a half always being supportive and always giving me all the affection that I needed.

A special thank to my friends and family for all the moments of support that they give me.

For last, I would like to thank to the Electronic, Telecommunications and Informatics Department of University of Aveiro and to the Institute of Telecommunications at Aveiro.

Palavras-Chave

Segurança, Auxílio Inteligente ao Condutor, Comunicações sem Fios, WiMAX

Resumo

Os acidentes rodoviários têm um enorme impacto na sociedade, quer devido às perdas humanas daí resultantes quer devido aos custos económicos a si associados. Por todo o mundo, esta situação levou ao estudo de mecanismos que permitem aumentar a segurança nas estradas. Por exemplo, na Europa estão a ser financiados vários projectos para desenvolver estes mecanismos e a maior parte das iniciativas em curso requerem a possibilidade dos veículos comunicarem entre si e/ou com estações que se encontram fixas junto à estrada. Devido aos requisitos de mobilidade dos veículos, as tecnologias de comunicação sem fios têm um papel crucial neste tipo de aplicações. Neste sentido, esta dissertação avalia a adequação da tecnologia de comunicação sem fios WiMAX para a transmissão de serviços de segurança rodoviária e/ou outros, entre os veículos e a infraestrutura, usando para isso os mecanismos integrados de diferenciação de tráfego desta mesma tecnologia de comunicação. Especificamente, o objectivo é avaliar se estes mecanismos são apropriados para fornecer os serviços atrás mencionados tendo em conta os seus requisitos tempo-real (largura de banda, latência, variação da latência, etc.).

Keywords Safety, Intelligent Driver Aids, Wireless Communications, WiMAX

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. This dissertation assesses the suitability of the WiMAX wireless technology for supplying vehicle to infrastructure road safety services and others, using this communication technology integrated quality of service mechanisms that provides traffic differentiation. Specifically, the purpose is to evaluate if these mechanisms are appropriate to provide the referred services taking in account their real-time requirements (bandwidth, latency, jitter, etc.).

Table of Contents

List of Figures

List of Tables

List of Acronyms

ABS	Anti-lock Breaking System
ACK	Acknowledgment
AES	Advanced Encryption Standard
AMC	Adaptive Modulation and Coding
API	Application Programming Interface
ARQ	Automatic Repeat Request
ASIC	Application Specific Integrated Circuit
BE	Best Effort
BPSK	Binary Phase Shift Keying
BS	Base Station
CBC	Cipher Block Chaining
CID	Connection Identifier
CINR	Carrier to Interference-plus-Noise Ratio
CLI	Command Line Interface
COOPERS	CO-operative Systems for Intelligent Road Safety
CP	Cycle Prefix
CPS	Common Part Sub-Layer
CRC	Cyclic Redundancy Check
CS	Convergence Sub-Layer
CVIS	Cooperative Vehicle-Infrastructure Systems
DCD	Downlink Channel Descriptor
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL-MAP	Downlink MAP
DSA	Dynamic Service Addition
DSC	Dynamic Service Change
DSD	Dynamic Service Deletion
DSRC	Dedicated Short Range Communication
ECU	Electronic Control Unit
ertPS	Extended Real-Time Polling Service
ESP	Electronic Stability Program
FCH	Frame Control Header
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FFT	Fast Fourier Transform

FP6	Sixth Framework Program
FTP	File Transfer Protocol
GPIO	General Purpose Input Output
GPS	Global Positioning System
H-FDD	Half Frequency Division Duplex
HARQ	Hybrid Automatic Repeat Request
HCS	Header Check Sequence
HTTP	Hipertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDE	Integrated Development Environment
IF	Intermediate Frequency
LMAC	Lower Medium Access Control
LOS	Line of Sight
MAC	Medium Access Control
MSDU	MAC Service Data Unit
NLOS	Non-Line of Sight
nrtPS	Non-Real-Time Polling Service
OBU	On-Board Unit
OFDM	Orthogonal Frequency Division Multiplex
OFDMA	Orthogonal Frequency Division Multiple Access
OS	Operating System
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
PKM	Privacy Key Management
PMP	Point to Multipoint
PS	Physical Slot
PSAP	Physical Service Access Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RCC	Regional Control Center
REQ	Request

RF	Radio Frequency
RSSI	Received-signal-strength-indication
RSP	Response
RSU	Road Side Unit
RTOS	Real-Time Operating System
rtPS	Real-Time Polling Service
SA	Security Association
SAP	Service Access Point
SDU	Service Data Unit
SF	Service Flow
SNMP	Simple Network Management Protocol
SoC	System on Chip
SPI	Serial to Parallel Interface
SS	Subscriber Station
TCS	Traction Control System
TDD	Time Division Duplex
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TEK	Encryption Key
TFTP	Trivial File Transfer Protocol
UART	Universal Asynchronous Receiver Transmitter
UCD	Uplink Channel Descriptor
UGS	Unsolicited Granted Service
UL	Uplink
UL-MAP	Uplink MAP
UMAC	Upper Medium Access Control
URI	Uniform Resource Identifier
USDOT	U.S. Department of Transportation
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VSC	Virtual Sub-Center
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 and has involved more than 47,000 people, killing 850 [1]. In the European context, in 2005 more than 40,000 people were killed in road accidents [2]. This scenario has a dramatic and unacceptable impact in terms of human life losses and injuries as well as in the economy. In pair with initiatives associated with driver behavior changes, 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. The development and deployment of such mechanisms can have a positive impact and can help to reduce the road fatalities and injuries.

1.2 . Road Safety and Vehicular Communications

In the last decades, a substantial effort has been devoted to study and develop mechanisms that improve road safety. The initial efforts have been directed mainly to improvements on in-vehicle subsystems and operate entirely based on local sensors and actuators. Examples are 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. However, these mechanisms are merely reactive, not being able to foresee potentially dangerous situations beyond their environment, and so, despite being extremely useful, exhibit a limited scope of coverage.

One of the approaches that can achieve a better scope of coverage and then enhance road and traffic safety is improving the sensing capabilities, allowing the drivers to be informed in advance of abnormal and potentially dangerous situations. This scenario becomes possible if drivers and vehicles can communicate with each other and with roadside base stations. Those mechanisms could have a major importance on many common but potentially dangerous daily road situations like reporting accidents, approach of traffic jams or other obstacles in highways, approach of emergency vehicles, lane changes, cross of highway intersections, etc. Consequently the drivers' radius of perception is effectively enlarged and so knowledge about potentially dangerous situations is anticipated, improving the capability of the driver in carrying out correct maneuvers and avoiding accidents.

Two possible communication architectures can be used to achieve these purposes: *Vehicle to Vehicle communication* (V2V) and *Vehicle to Infrastructure communication* (V2I). The V2V communication consists on the transmission of road safety information between vehicles on the road and V2I communication consists in using a fixed road side station to communicate with the vehicles in order to transmit safety information (sometimes the I2V term is used to characterize the communication from the infrastructure to vehicles). This document is focused on the V2I communication system that is composed by: the *On–Board Unit* (OBU) and *Road–Side Unit* (RSU). The OBU is the unit that resides on each vehicle and that allows the communication with the RSU that is a unit on the side of the road which can send safety related information or other to the OBU (Figure 1).

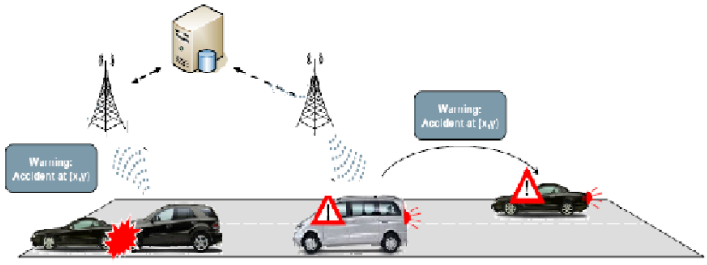

Figure 1: Coexistence of V2I and V2V [3]

The mobility constrains associated with these two vehicular communication architectures open a door to the usage of wireless technologies. Several of them, like GSM, GPRS, WiFi, BlueTooth,

Dedicated Short Range Communications (DSRC) and others can and have been explored to perform V2I communication. The V2I applications require a communication system capable of providing information to the vehicles on the road taking in account requirements such as bandwidth, maximum latency, jitter, timeliness and coverage area.

1.3 . WiMAX as Vehicular Communication Candidate

One of these technologies that, to our best knowledge, was not yet adequately explored in this type of applications is WiMAX, which has promising features (e.g., range, bandwidth and real-time guarantees) for implementing V2I/I2V communication and therefore is a candidate to be evaluated. WiMAX, the Worldwide Interoperability for Microwave Access, is a standards-based wireless technology, based on the IEEE 802.16 [4] standard 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 [5]. With this technology it is possible to have Quality of Service (QoS) in the Medium Access Control (MAC) layer. It is also possible with WiMAX to have bidirectional communication with configurable percentage of transmit/receive time (in time division duplex mode – TDD). So, this technology could be used for some specific vehicular applications like the following ones:

1. Safety Warning: The driver could get messages about dangerous situations that he/she is about to face;
2. Assisted Driving: The driver could be helped and assisted in order to take the correct behavior when facing a potential dangerous situation;
3. Traffic Management: The V2I communication could be used to avoid or solve traffic jams informing drivers not to go along the problematic areas.
4. Commercial Applications: video, music, and others.

1.4 . Objectives and Document Outline

This dissertation introduces WiMAX as a vehicular communication technology, concretely in V2I/I2V communication, and discusses its suitability to support the application domains above identified. It is the main objective to study the timing requirements of several vehicular applications and to understand the impact of the introduction of road safety services on a WiMAX equipment developed on WiRIA project where the author is collaborating. It will be performed a study on the impact of the introduction of these services on the WiMAX equipments scheduling and try to understand which safety services can be addressed by these equipments, taking in account real-time requirements like latency and jitter.

The work that is being performed is related to the WiRIA project that aims to project, develop and test a WiMAX Subscriber Station (SS) to operate with a commercial WiMAX Base Station. This project is funded by TELESAL and is coordinate by Institute of Telecommunication, University of

Aveiro and PT Inovação. The work performed to assess WiMAX as a vehicular communication technology is also funded by BRISA, S.A. A paper, which title is "Assessing WiMAX for vehicular communications", related with the work performed on this dissertation was already accepted for presentation at the CONTROLO'2008 - The 8th Portuguese Conference on Automatic Control to be held in Vila Real, Portugal from 21 to 23 July 2008.

The remaining of this document is organized as follows: Chapter 2 presents a brief survey on the state-of-the-art of V2I and V2V, with particular focus on European projects; Chapter 3 provides some background information on the WiMAX wireless technology; Chapter 4 shows the WiMAX development platforms that were studied in order to develop the WiMAX SS; Chapter 5 provides a explanation about the hardware/software architecture provided with the WiMAX development kit chosen; Chapter 6 presents the new software architecture developed to create a real WiMAX SS solution; Chapter 7 presents the specific V2I applications studied and their requirements followed by the specification and results obtained from several tests performed using WiMAX technology; Chapter 8 presents the conclusions of the work performed and propose future work to be done in this context.

Chapter 2

State-of-the-art

The concern of reducing road injuries and fatalities is present all over the world and therefore many initiatives are being developed to pursue this objective. So, a large number of projects related to road safety are currently under way, mainly in the USA, Japan and Europe, and almost all of them use V2V and V2I communications as ways of achieving a road accidents reduction. In this chapter, the focus will be mainly directed to the European projects that are being funded by the European Commission.

2.1 . Introduction

All over the world, many initiatives are being deployed with the purpose of reducing car accidents on the roads. To achieve this objective, it is necessary to supply specific safety services using V2V

and V2I communication architectures. Some of these services can be provided using both V2V and V2I communication systems but others present constrains that require using one specific architecture. Typically, safety services related to static dangerous situations such as narrow curves, tunnels, bridges, work on the road or bad weather conditions can be addressed using V2I communication because the infrastructure intrinsically knows their dangerousness. On the other hand, information about dangerous situations that appears suddenly such as a sudden car break, formation of ice on the road or the approximation of priority vehicles can be shared among vehicles using a V2V architecture to provide safety warnings to the vicinity as soon as possible.

All of the services described above present requirements of mobility, reliability and timeliness in order to be useful and then improve safety on the roads. In the following sections, there are presented some on-going projects that have the objective to fulfill the requirements identified using different approaches to address road safety issues.

2.2 . European Projects

The European Commission and the automotive industry are strongly committed to improve road safety and reduce the number of accidents in European roads. The initiative eSafety [6] reflects this will "*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 [6]. Associated with the eSafety initiative is the eSafety Forum [2], which has the objective of promoting and monitoring the implementation of the recommendations identified by the eSafety Working Group, as well as support the development, deployment and use of new and intelligent integrated road safety systems. Since 2002, this initiative has funded a number of projects, where the V2V and V2I are the base of several of them.

So, as referred before, the European Commission is funding several projects that use information and communication technologies in intelligent solutions, in order to increase road safety [7]. The projects funding is currently (November 2007) done 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 [8].

2.2.1. COMeSafety

The COMeSafety project [9] has been funded with 1.1M€ and 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 depicted in Figure 2.

COMeSafety provides a platform that allows the exchange of information and the presentation of results among the entities shown in Figure 2. Regular electronic newsletters and publications at major conferences and press events complement the dissemination efforts. For European and

worldwide harmonization, liaisons are established and workshops are organized to bring together the eSafety Forum and all stakeholders. COMeSafety provides an open integrating platform, aiming for the interests of all public and private stakeholders to be represented. [9]

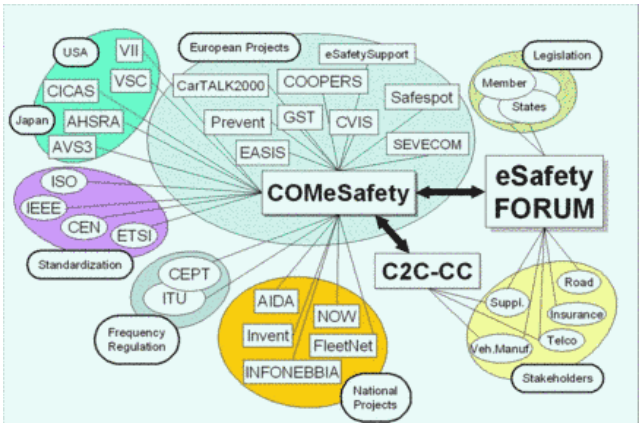

Figure 2: COMeSafety projects Network [9]

2.2.2. COOPERS

The *CO-operative Systems for Intelligent Road Safety* (COOPERS) project [10] is funded with 9.8M€ by FP6 and has the ambition to connect vehicles to road infrastructures on motorways. This link will allow the exchange of data and information to increase the safety in specific road segments (Figure 3). The V2I communication in this respect will significantly improve traffic control and safety via effective and reliable transmission of data fully adapted to the local situation of the vehicle (ensemble of vehicles) as depicted in [10].

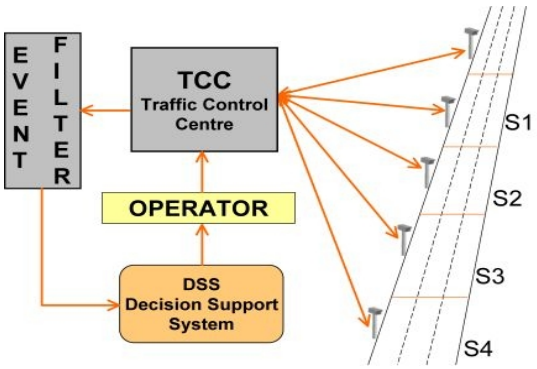

Figure 3: COOPERS vision [10]

COOPERS follows a 3-step approach for implementing V2I communication: improvement of road sensor infrastructure and traffic control applications for more precise situation based on traffic information and driver advisement; Establishment of a link between road tolling systems and V2I concept; Development of a communication concept and applications able to cope with the V2I requirements in terms of reliability, real time capability and robustness [10].

So, the mission is to define and develop services and equipment to provide bi-directional links between the infrastructure and vehicles (V2I) using **an open standardized wireless communication technology**. A stable link needs to be established in order to ensure the transmission of real-time location-based safety related information on the current traffic status [10]. 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 [10].

2.2.3. SAFESPOT

The SAFESPOT project [11] is also funded by FP6 with 20.59M€ and has the purpose of preventing road accidents developing a "Safety Margin Assistant" that detects in advance potentially dangerous situations and extends "in space and time" drivers' awareness of the surrounding environment. The Safety Margin Assistant will be an Intelligent Cooperative System based on V2V and V2I communication. It 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 and develop a new generation of infrastructure-based sensing techniques.

The specific objectives on SAFESPOT project are to improve the range, quality and reliability of the safety-related information available to 'intelligent vehicles' by providing "extended co-operative awareness" through the real time reconstruction of the driving context and environment, to support drivers preventively to the proper manoeuvres in the different contexts, to optimize the intervention of vehicle controls with respect to critical situations, to manage existing incidents to minimize further negative safety impact, to open the development of new safety applications based on the cooperative approach and to increase the safety for all road users (including pedestrians and cyclists).

SAFESPOT defines 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; these road scenarios are typically addressed by V2I communication.
2. **Dynamic black spots** or "**dynamic risky conditions**", which are where the driving scenarios may become unexpectedly and suddenly dangerous (like ice conditions, a queue behind a curve, a vehicle that suddenly harshly breaks, presence of vehicles in blind spots, etc.). This type of scenarios are typically addressed using V2V and V2I communication.

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.

2.2.4. CVIS

The *Cooperative Vehicle-Infrastructure Systems* [12] project aims to design, develop and test new technologies needed to allow vehicles to communicate with each other and with **the nearby roadside infrastructure**. The main objective is to create standardized in-vehicle and roadside modules capable of communicating continuously and seamlessly using a wide range of communication media, including mobile cellular and wireless local area networks, short-range microwave (*Dedicated Short Range Communications* - DSRC) or infrared (Figure 4).

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 CVIS. To achieve these objectives CVIS will build on **the latest global communication standards** to develop its world.

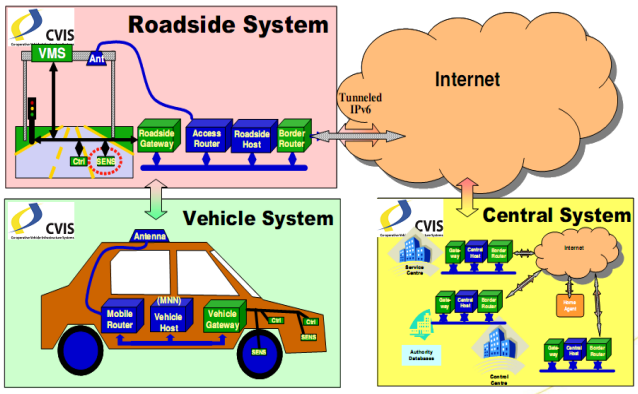

Figure 4: CVIS communication concept [12]

2.2.5. COM2REACT

Another FP6 funded project with 3M€ is COM2REACT [13]. Its vision 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 [13].

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 5). 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. The role of VSC is set, unnoticeable by the driver, to one of the vehicles in the group according to rules embedded in all COM2REACT vehicles. It is also wanted **to adapt existing communication technologies** to perform these communications (ex. WiFi, GPRS) [13].

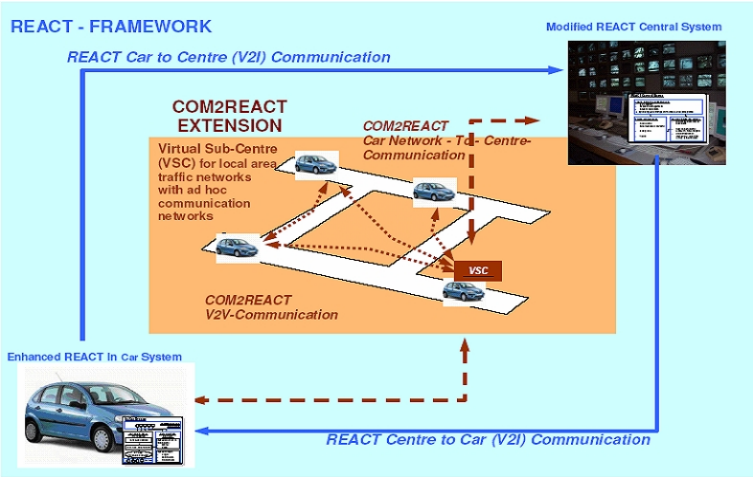

Figure 5: COM2REACT three level architecture [13]

2.3 . Other European Projects

There are other European projects funded by FP6 that have the purpose of improving road safety and reducing injuries and fatalities. All of them relies on the concept of vehicular communication and accept that V2V and V2I communication will be a central part on the road safety system in the future. For example, one of the objectives of the PReVENT Integrated Project [14] is to develop, demonstrate, test and evaluate preventive safety applications, using advanced sensor, **communication** and positioning technologies integrated into on-board systems for driver assistance and then communication technologies are needed to improve the detection, location and evaluation of hazards [14]. There are also projects that want to solve security issues in vehicular communications like SEVECOM project [15]. This project has the vision that vehicular communication and inter-vehicular communication bring the promise of improved road safety and optimized road safety and then aims to identify a variety of threats to vehicular network, to specify an architecture, security mechanisms and cryptographic primitives to be used in vehicular networks.

Beside the European projects referred in this document there are much more (some of them funded by FP6 and some don't) currently under way and that want to address road safety. Looking at them we can find a common thought: **vehicle to vehicle communication and vehicle to infrastructure communication will be an essential part of the road security systems in the future**.

2.4 . More Initiatives

The effort of improving road safety is not present only in Europe. There are also a lot of initiatives mainly in the United States of America and in Japan that aims to reduce road injuries and fatalities. For example, in the USA, this promise is being carried out mainly by the *U.S. Department of Transportation* (USDOT) and some partners. Projects like VII [16] defines the establishment of V2V and V2I communication capability nationwide and has the purpose to enable a number of new services that provide significant mobility, safety and commercial benefits.

2.5 . Conclusion

The brief survey on eSafety projects above presented permits concluding that the wireless communication technologies will be at the center of all road security systems in the future. Until now, several research directions have been pursued in this domain. Some projects are addressing the possibility of using standard technologies, such as Wi-Fi, BlueTooth, GSM or UMTS while others are focusing the development of custom technologies, eventually derived from standard ones (DSRC).

The initiatives that are studying standard technologies or derived to perform vehicular communications face several challenges when trying to supply safety vehicular services. These challenges are related to the specific requirements of this type of communication scenario: (1) **mobility**: the relative position between the vehicles and road fixed station varies during the transmission; (2) **timeliness**: it is necessary to guarantee that the safety information is delivered to vehicles in appropriate times to not compromise its usefulness; (3) **coverage area**: with an extended coverage area it is possible for the information transmitted to reach vehicles sooner decreasing the number of RSU's needed and associated costs and (4) **bandwidth**: it is important to guarantee enough bandwidth to provide several simultaneous safety services to the vehicle in a certain coverage area.

The standard technologies were not projected for this type of application and therefore present some weaknesses in some of the requirements above identified. For example, DSRC (based on WiFi) presents a large available data rate (bandwidth) that can reach 27 Mbps but has a small/medium coverage area (1000m maximum) then increasing the number of RSU's needed and associated costs. BlueTooth present a small coverage area (can reach 100m for class 1) and a low data rate that can only reach 3 Mbps despite of existing new proposals for increasing it. Cellular networks like GSM or UMTS present a large coverage because they are widely deployed, however they present a small available bandwidth that can reach only 10 Mbps (theoretically) in the better case (UMTS).

So, it is possible to see that none of the standard or derived technologies mentioned matches perfectly the V2I applications requirements and that, until now, no clear winner has emerged, and so the assessment of wireless technologies is still an open issue. In this way, WiMAX can also be a candidate to perform V2I communication because some of its features seem to be suitable to supply

this type of applications: the coverage area of WiMAX can reach tens of km in an LOS environment providing data rates of 20 Mbps (using a 7MHz channel bandwidth). However, the characteristic that distinguish the most this technology from the other ones is the fact it has QoS mechanisms implemented in the MAC layer that allow to have traffic differentiation. So, it is possible to prioritize time critical information services without the necessity of implementing further mechanisms. Therefore, WiMAX seems to have the necessary characteristics to be evaluated as a possible solution for V2I communication.

Chapter 3

Overview of WiMAX

WiMAX, the Worldwide Interoperability for Microwave Access, is a telecommunication technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. This technology has some extremely promising characteristics, such as the support of different QoS levels and traffic classes, including real-time guarantees, high range and bandwidth, and thus it is a strong candidate for V2I communication. The reminder of this section presents a brief characterization of the WiMAX technology and the 802.16 standard in which is based on.

3.1. Background

The IEEE 802.16 [17] group was formed in 1998 to develop an air-interface standard for wireless broadband [18]. This group initial objective 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 physical (PHY) layer with a burst time division multiplexed (TDM) MAC layer. Subsequently, the IEEE 802.16 group produced the 802.16a amendment, to include Non-LOS (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 [19], replaced all prior versions and formed the basis for the first Fixed WiMAX solution [20]. In December 2005, the IEEE group completed and approved IEEE 802.16e-2005 [21], an amendment to the IEEE 802.16-2004 standard that added mobility support, which forms the basis for the Mobile WiMAX [22].

The WiMAX Forum [23] 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 [20]. A WiMAX Forum goal is to accelerate the introduction of these systems into the marketplace [20]. The WiMAX Forum has also established some profiles for certification. There are different 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 then interoperability.

3.2. Fixed and Mobile WiMAX: Main Features

As stated in previous section, WiMAX wireless technology has two different versions: Fixed and Mobile. These two versions are targeted for different applications and despite of having several similarities they present some technical differences. Their features are presented in a brief survey next, mentioning which are the main differences between them when necessary [18]:

- **OFDM-based physical layer** - scheme that offers a robust behavior in presence of multipath radio signal propagation, allowing WiMAX to operate in NLOS conditions.
- **Orthogonal frequency division multiple access (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.
- **Support for TDD and FDD** - the WiMAX supports time division duplexing (TDD), frequency division duplexing (FDD) and Half-FDD.
- **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 physical-layer architecture that allows for the data rate to scale easily with the available channel bandwidth. This scalability is supported in the OFDMA mode (Mobile WiMAX), where the FFT size may be scaled based on the available channel bandwidth. This is not applicable for fixed WiMAX.
- **Adaptive modulation and coding (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 retransmission requests (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-ARQ, which is an effective hybrid between FEC and ARQ.
- **Flexible and dynamic per user resource allocation** - Both uplink and downlink 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.
- **Quality-of-service 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 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 handover 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. Physical-layer 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-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.

3.3. Basic Topology

The IEEE 802.16 standard defines two different basic topologies: Point-to-Multipoint (PMP) and Mesh but only the first one is used in the WiMAX technology. This kind of topology consists in two logical entities: the Base Station (BS) and the Subscriber Station (SS) [24]. In this case, the BS and SS are in a master-slave relationship, where the SS must follow the medium access rules defined by the BS (Figure 6). It is important to refer that all the communications are always performed between a BS and SS and vice-versa.

The 802.16-2004 technology is exclusively connection-oriented. Therefore, all transmissions are based on a connection and no packets are allowed to traverse the wireless link without a specific connection being previously allocated. A connection is, by definition, a unidirectional mapping

between the BS and the SS MAC layers for the purpose of transporting service flows traffic. To uniquely identify a connection, a 16-bit *Connection Identifier* (CID) is used [25].

The transmission performed by the BS (downlink) and by the SS's (uplink) can be done at the same time in different frequencies or at different times in the same frequency. The first one is called *Frequency Division Duplex* (FDD) and will be not explored in this study because it brings more hardware complexity (two radio modules necessary). The second one is *Time Division Duplex* (TDD) and the transmission done by the BS and SS's are at the same frequencies but occur in different times. Therefore there is always a defined time to the downlink transmission direction (downlink sub-frame) followed by an uplink transmission time (uplink sub-frame) like shown in Figure 7. The downlink sub-frame and uplink sub-frame form the transmission frame and its duration is fixed. However the time duration of the downlink and uplink sub-frames are adaptive.

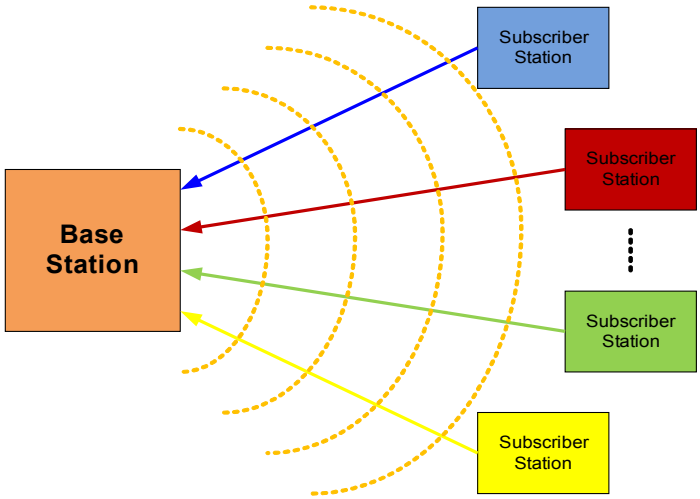

Figure 6: PMP Topology

The BS transmission is done in a *Time Division Multiplex* (TDM) fashion providing information to each registered SS in different times in the downlink sub-frame. In this type of topology there is only one BS and therefore all SS's registered in this BS receive all transmissions. So, each SS needs to select the information which is directed to it discarding the other. This selection is performed by inspecting the *Connection Identifier* (CID) of each MAC *Protocol Data Unit* (PDU) sent. On the other hand, the transmission done by the SS's is performed on a *Time Division Multiple Access* (TDMA), that is, in each moment only one SS can transmit and those moments are granted by the BS. These BS grants are based on the scheduling service associated to each flow of packets implementing, in this way, service differentiation. This type of communication is commonly known as Master – Slave communication.

In order to perform the communication explained above it is necessary to control the access to the medium (air) by all the network entities defining the rules to be followed on each transmission. It is also necessary to implement mechanisms that make the transmissions reliable, i.e., that give some

assurance that the information transmitted reaches its destination and that the receiver can understand it. The network layers defined in the IEEE 802.16 address those issues.

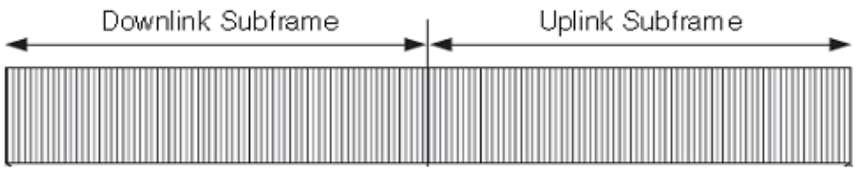

Figure 7: TDD Duplexing

3.4. Network Layering

The 802.16 standard in which WiMAX is based defines both the *Medium Access Control* (MAC) and *Physical* (PHY) layers. The protocol stack is depicted in Figure 8. It is possible to see that the MAC layer is divided in three sub-layers: (1) The Convergence Sub Layer that is responsible for interfacing the MAC layer with the higher network layer performing all operations related to it; (2) The Common Part Sub Layer that performs all the more important MAC functions and (3) the Security Sub Layer that is responsible for all issues related to encryption and authentication. Below the MAC Layer there is the PHY Layer that performs the necessary operations to transmit reliably the information over the air.

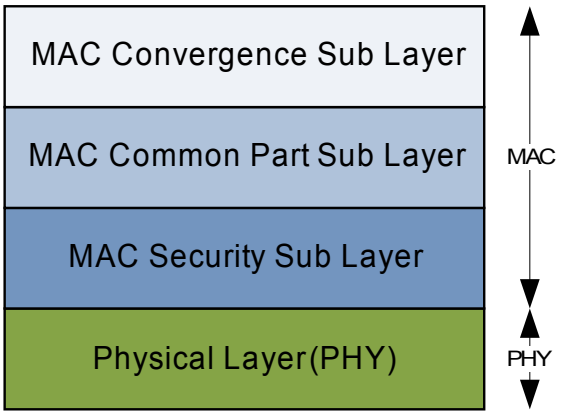

Figure 8: IEEE 802.16 Network layer

3.4.1. Physical Layer

The PHY Layer is responsible for accepting the data bursts from the MAC Layer performing several operations on it like *Forward Error Correction* (FEC) and modulation and creating the symbols to be sent over the air (it is also responsible to perform the reverse process when receiving data from the air).

Before explaining some of the processes executed in the PHY it is important to refer that the IEEE 802.16 standard defines four different PHY Layers: (1) WirelessMAN SC (11 – 66 GHz); (2) WirelessMAN SCa (2 – 11 GHz); (3) WirelessMAN OFDM (2 – 11 GHz) and (4) WirelessMAN OFDMA (2 – 11 GHz). However the WiMAX technology uses only two of them: WirelessMAN OFDM for the Fixed WiMAX and WirelessMAN OFDMA for Mobile WiMAX and therefore those are focused on this section.

When the OFDM or OFDMA PHY Layer receives MAC data through the PHY *Service Access Point* (SAP) it first performs the operations depicted in the transmission chain (Figure 9).

It is possible to see the different processes done by the PHY Layer. The randomization block is useful to avoid long sequences of consecutive ones or zeros. Then the randomized information is sent to the FEC encoder that consists in applying convolutional codes to the information (different mandatory codes for WirelessMAN OFDM and WirelessMAN OFDMA) and after this, the information is sent to the interleaving block that gives protection against long sequences of errors which are difficult to correct in the receiver. Then the repetition block (only present in WirelessMAN OFDMA) increases the signal margin further over the modulation and FEC mechanisms and for last, modulation is performed. The modulation is one of the four digital modulation used in WiMAX (BPSK, QPSK, 16QAM and 64QAM). It is the MAC Layer that controls which modulation should be used for each burst.

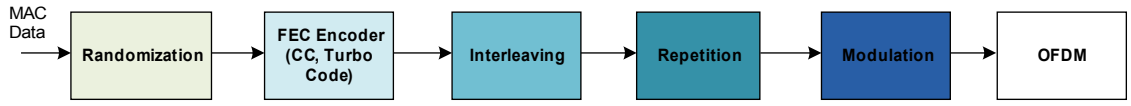

Figure 9: PHY Transmission Chain

After the modulation block, the information is sent to a stage related to the construction of the OFDM symbols that give protection against multipath transmission problems and then OFDM symbols are grouped to form the frame that will be sent over the air. It is important to say that the basic unit of time is the *Physical Slot* (PS) and that corresponds to four OFDM symbols. If the duplexing mode used is FDD then there will be a frame for the uplink and another for the downlink having the same time duration. However if TDD duplexing mode is used then there will be only one frame and this one will be divided in two sub-frames: downlink and uplink (see Figure 7). The uplink and downlink sub-frames are different for OFDM and OFDMA. In Figure 10 it is possible to see the OFDM downlink sub-frame constitution.

The preamble is used to synchronize the SS's that want to read the downlink frame. The *Frame Control Header* (FCH) is one OFDM symbol long and is transmitted at the more robust profile (BPSK ½) and then all downlink bursts are transmitted. The broadcast messages are the first to be transmitted followed by the multicast or unicast bursts in a decreasing order of robustness. The uplink sub-frame (Figure 11) is constituted by two contention slots where collisions can happen: initial ranging and bandwidth request. The first is used by the SS's to join the network and the

second is used by the SS's to send bandwidth requests to the BS. After these two slots, all the uplink bursts are sent to the BS, one for each SS. The two contention slots and uplink bursts are known by the SS's because this information is previously sent by the BS in broadcast messages.

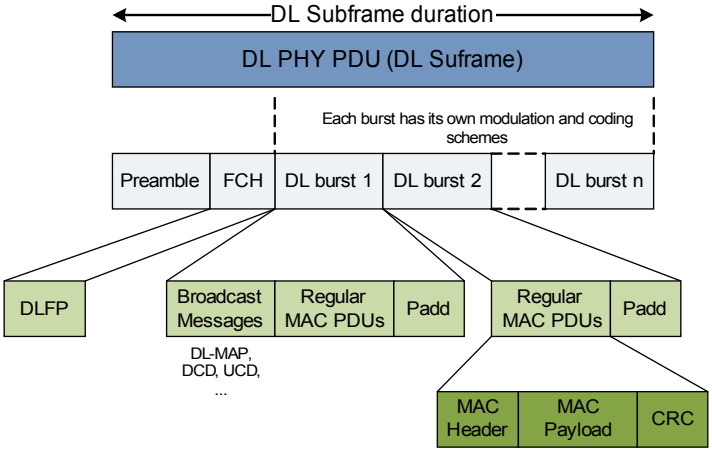

Figure 10: Downlink sub-frame constitution

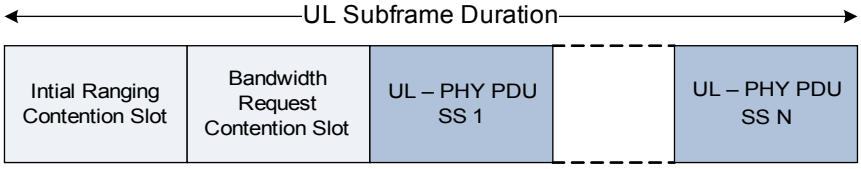

Figure 11: OFDM Uplink Subframe

3.4.2. MAC Security Sub-Layer

The MAC Security Sub-Layer provides authentication and data encryption functions. These functions afford privacy to subscribers and protect operators from theft of service. Their purposes are achieved by encrypting the data between the BS and SS using the *Privacy Key Management* (PKM) protocol.

In the sending entity, the MAC PDU's are mapped to a *Security Association* (SA) that defines the encryption processing to be done. In the receiving entity the reverse process is done after determining the CID and SA. An SA is a set of security information that is shared between the BS and SS using the PKM protocol. Some of the information included in the SA is the cryptographic suite to use, the encryption keys (TEK's) along with their lifetime. Only the payload of MAC PDU is encrypted.

The standard defines two cryptographic suites to be used: *Data Encryption Standard* (DES) in *Cipher Block Chaining* (CBC) mode and *Advanced Encryption Standard* (AES) in *Counter with CBC – MAC*

(CCM) mode. The first one provides a security that is not very strong because the keys are too short to be secure. The second one is considered to be more secure since the keys are longer. There are also processes to perform key management and certain rules need to be followed by SS's and BS's to solve security issues but they will be not explored in this document.

So, the MAC Security Sub-Layer is responsible to encrypt the payload of the MAC PDU's and to provide the mechanisms to manage all the security information shared between the SS and the BS.

3.4.3. MAC Common Part Sub-Layer

The CPS is the second sublayer from the MAC layer. It receives packets arriving from the *Convergence Sub-Layer* (CS) and it is responsible for a set of functions, such as addressing, construction and transmission of the MAC PDU's, implementing the uplink scheduling services, bandwidth allocation, request mechanisms, contention resolution, among others. The 802.16-2004 MAC is connection oriented since all services are mapped to a connection. Associated with each connection is a *service flow* (SF). Service flows provide a mechanism for uplink and downlink QoS management. [25]

The first concept that needs to be introduced is the 802.16 connection. A connection is an unidirectional mapping between the BS and SS identified by a CID. Therefore all MAC tasks are performed based on a connection except in the initial ranging and authentication processes. In the initialization process, three pairs of management connections (each pair has an uplink and a downlink connection) are established for each SS: (1) the basic connection that is used for short and time critical MAC management messages, (2) the primary connection that provides a way to transport longer and delay tolerant MAC management messages and (3) the secondary management connection to transfer standard-based management messages (optional). Other connections can be established after like broadcast, multicast polling or transport connections. The broadcast connection is used to send management messages to all SS's, the multicast polling connection is used by the SS's to join multicast groups and request bandwidth, and the transport ones are used to users traffic.

The MAC Layer is responsible to construct each MAC PDU associated with a certain connection. The MAC PDU format is depicted in Figure 12. It consists in a fixed-length header, a variable length payload and an optional C*yclic Redundancy Check* (CRC) field. The MAC header can assume two different formats defining that way two different types of MAC PDU: (1) Generic MAC Header or (2) Bandwidth Request Header.

Figure 12: MAC PDU format

The Generic MAC Header is used by MAC PDU's that transport data coming from the CS layer (users data) or MAC management messages and consists in a MAC Header with the payload and a CRC field. When a MAC PDU is built with information coming from the CS layer then a MAC SDU can be divided in several MAC PDU's (fragmentation) or several MAC SDU's can be grouped in one MAC PDU (packing). It is also possible to agglomerate several MAC PDU's to be transmitted in the same burst (concatenation). The Bandwidth Request Header is used by the SS's to request additional bandwidth and shall not have any payload nor CRC field.

The MAC management connections established in the initialization process (broadcast, basic, primary, ...) transmits only MAC management messages. Those messages are transported in the payload of a Generic MAC PDU and consist in a type field followed by MAC management payload field. The standard defines several management messages and next some of the more important are described:

- Downlink Channel Descriptor (DCD) and Uplink Channel Descriptor (UCD)
- Downlink MAP (DL-MAP) and Uplink MAP (UL-MAP)
- Dynamic Service Addition Request (DSA-REQ), Response (DSA-RSP) and Acknowledgment (DSA-ACK)
- Dynamic Service Change Request (DSC-REQ), Response (DSC-RSP) and Acknowledgment (DSC-ACK)
- Dynamic Service Deletion Request (DSD-REQ)

The DCD and UCD are sent periodically by the BS to SS's in order to provide the channel downlink and uplink characteristics respectively. The DL-MAP and UL-MAP messages are also sent periodically by the BS to provide information about the access to downlink and uplink information defining the access to the medium. The DSA, DSC and DSD messages are used to create, change or delete *service flows* (SF) for user's traffic.

Associated with each SF created using DSA messages there is the scheduling service. In the IEEE 802.16-2004 (Fixed WiMAX) there are four different scheduling policies that can be assigned to a SF and that defines its QoS: *Unsolicited Granted Service* (UGS), *real-time Polling Service* (rtPS), *non-real-time Polling Service* (nrtPS) and *Best Effort* (BE). The IEEE 802.16e-2005 added one more scheduling service: *extended real-time Polling Service* (ertPS).

- The UGS policy is used for fixed length periodic real time data streams. In this type of service, the BS gives data grants at periodic intervals so the SS's do not need to perform a request for bandwidth thus eliminating latency and overhead. The size of the grants is sufficient to hold the fixed-length data associated with the service flow.
- The rtPS scheduling policy is used to real-time streams that have a variable length and are sent at periodic intervals. The BS provides unicast request opportunities for the SS to request data grants of a specific size. This scheduling service has more overhead that UGS and allows to have a variable packet size improving efficiency for services like MPEG.

- The nrtPS is used for streams tolerant to delay and that have a variable data packet size. The BS provides unicast uplink request opportunities on a regular basis (one second or less). This service is also authorized to use contention request opportunities.
- The ertPS service provides an efficiency that relies on the UGS an rtPS services. The BS provides unicast grants like UGS but the allocated grant size is dynamic like the rtPS protocol.
- The last scheduling service is Best Effort. This kind of service is used by the streams that don't have any requirements. The BS has no obligation to issue request opportunities to CID's associated with a BE service so it is possible to pass a long time before getting any bandwidth.

The scheduling services described in the previous paragraph provide service differentiation because they are treated by the BS differently. It is possible to see that the impact of scheduling services is mainly done on the uplink direction because it is the BS that gives bandwidth to the SS's. The main difference between the scheduling services is in the way that they can ask for bandwidth and how this bandwidth is given by the BS (the BS scheduler decides to which SS the bandwidth is granted). For example, SS's that have UGS connections doesn't have to request bandwidth in order to be given time to transmit.

When an SS needs to request more bandwidth to the BS it can use a Bandwidth Request Header described previously or a PiggyBack Request using a special sub-header. Those requests are done on a connection basis. However the bandwidth grants given by the BS are allocated to the SS's. So, the scheduler in the SS needs to decide to which connection the bandwidth will be given. If a connection has done a request and didn't have received any bandwidth then it repeats the request according to a back off algorithm. In order to send bandwidth requests, the SS's are allocated bandwidth. This process is called polling and the bandwidth can be granted to a specific SS (unicast polling) or to several SS's (multicast polling). When the polling is multicast it is necessary to have a contention resolution algorithm since collisions can occur. There is another polling process that is performed when SS's that have UGS connection explicitly ask to be polled in order to request bandwidth for non UGS connections.

The standard doesn't define multicast or broadcast connections to users' traffic, only for polling or management messages. To achieve that, it is necessary that the BS starts to associate and allocate a regular transport connection to a specifics SS and then assign this same connection, identified by its CID, with the SS's that will be part of the multicast group or to all SS's if broadcast. Other processes need to be controlled by the MAC CPS layer like the *Automatic Repeat Request* (ARQ) that retransmit MAC PDU's if they are not acknowledge by its receiver.

3.4.4. MAC Convergence Sub-Layer

The CS Sub-Layer resides above the MAC CPS Sub-Layer and is responsible to perform all the operations related to higher level protocols. In the transmitter side it should transform a PDU from

a higher layer protocol into an MAC *Service Data Unit* (SDU) and assign each MSDU to a particular connection. In the receiver it should perform the inverse operation. It is possible to suppress some header information from the higher layers PDU's in this sub-layer. The IEEE 802.16 standard defines two different CS sub-layers to use: ATM CS and Packet CS. WiMAX technology uses only the Packet CS so this is the one that will be explained next.

As explained before, the CS sub-Layer is responsible for receiving the PDU's from the higher layers through the CS SAP, perform some specific operation creating the MSDU and then deliver it to the MAC CPS Sub-Layer through the MAC SAP like depicted in Figure 13. The main operations performed in this sub-layer are:

– **Classification**: consists in determining in which MAC connection a particular packet shall be carried;
– **Payload Header Suppression (PHS)**: consists in removing the repetitive part of the higher layer packets header (optional);

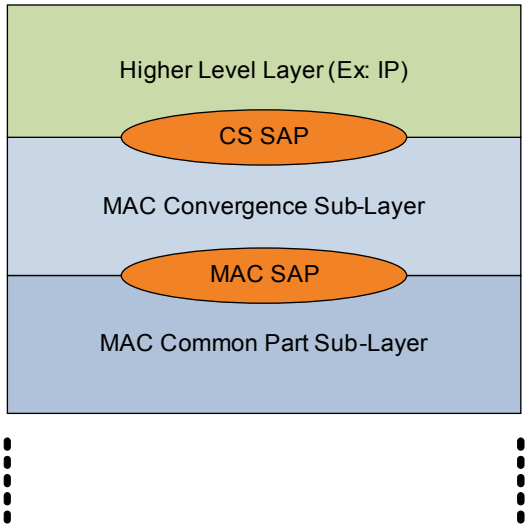

Figure 13: Convergence Sub-Layer Service Access Points

Classification is the process in which the MAC SDU's are associated with a connection to exchange traffic between MAC peers. This mapping allows MAC SDU's to be associated with the connection as well as with the service flow and QoS parameters. A classifier is a set of criteria dependent of the higher level protocol (for example IP address), a priority and an associated CID and they are applied to all the packets that enters the 802.16 network. If the packet matches to a criteria then it is delivered to the associated SAP to be sent in the connection identified by the CID. The service flow characteristics in which the connection is associated defines the QoS parameters for the information. The classifier priority is used only to know what classifier should be used when two distinct classifiers can be applied to the same packet. If no criteria could be applied then the packet should be dropped.

If PHS is active for a certain connection then the BS and the SS need to negotiate some parameter when the connection is created. Those parameters are [24]:

- **Payload header suppression index (PHSI)**: index to the PHS rule to apply to a packet;
- **Payload header suppression field (PHSF)**: string of bytes containing the information allowing the receiver to reconstruct the suppressed information in each packet;
- **Payload header suppression mask (PHSM)**: string of bits, each corresponding to a byte in the PHSF. If a bit is set then the corresponding byte is suppressed in the sender and reconstructed in the receiver;
- **Payload header suppression size (PHSS)**: parameter indicating the total number of bytes to be processes by the PHS;
- **Payload header suppression valid (PHSV)**: boolean value indicating whether the sender will compare the actual packet header with the version as it will be reconstructed by the receiver.

The PHS rule to apply to each packet is determined by the sender based on the classification established and the receiver can rebuild the packet by inspecting the PHSI and CID associated with each packet.

3.5. Network Boot and Initialization Process

This subsection describes the procedure carried out when an SS enters the network. So, once the SS is powered up, it begins the boot and initialization process. In a PMP topology, this process consists in the following 8 steps [24]:

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 transmission parameters through broadcasted messages sent by the BS.
3. **Initial Ranging –** this process has the finality of adjusting the transmission power for optimal BS reception, allocating the SS basic and primary management connections identifiers (CID's); and, for FDD and Half-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 associations (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. **Establish 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 processes optional.
8. **Establish 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.

3.6. Summary

This section presented a brief overview of WiMAX starting with an historical background of the IEEE 802.16 standard and WiMAX technology followed by a survey of the main features of WiMAX. Then the network topology was explained starting with the PHY Layer followed by the three MAC Sub-Layers: Security Sub-Layer, CPS Sub-Layer and CS Sub-Layer. The MAC layer is totally connection-oriented, therefore, a classification mechanism must be used to classify each incoming packet in the system into one of its specific connections. This task is done by the CS, which classifies the incoming packets and delivers them to the correspondent connection. The CPS is responsible for the addressing and connection creation mechanisms, while the privacy sublayer is responsible for the security-related issues. Last, a description of the SS network entry process was presented.

Chapter 4

WiMAX Unit Development Kits

As stated in Chapter 2, a V2I architecture requires the communication between vehicles and the infrastructure using OBU's and RSU's. In this context, the RSU role is performed by a WiMAX BS that controls the medium and manages the dissemination of safety related information to the vehicles within its coverage area. Conversely, the OBU's are supported by WiMAX SS's, having the role of detecting the presence of RSU's, engaging in the network and performing the information exchange with the RSU. The communication channels are bidirectional, thus allowing the OBU to send information to the RSU informing the infrastructure about potentially dangerous situations that were perceived.

In order to study and perform a real-time analysis of WiMAX equipments with the purpose of using this technology in vehicular communication scenarios, it is necessary to have access to a WiMAX unit software and hardware. So, this study is related with the WiRIA project, where the author is currently collaborating, coordinated by Portugal Telecom Inovação, University of Aveiro and Institute of Telecommunications [27] that has the objective to project, develop and test a

WiMAX SS for the fixed WiMAX version. The developed SS should be operable with a commercial BS (AN-100U) from Redline Communications company [37]. So, to develop a WiMAX SS it was necessary to study and choose a development platform to accelerate the construction of such device.

4.1. WiMAX Development Platforms

In the scope of the WiRIA project, a market research of WiMAX development platforms was performed with the purpose of finding the solution that best fits to the WiRIA project needs. The points that were considered in this study were the standard compatibility and certification (802.16d, 802.16e or both), the type of device that can 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 as well as associated costs (free or proprietary, price, royalties feeds, ...), 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.

4.2.1. ASPEX WiMAX Development Kit

The ASPEX semiconductor [28] company provides a WiMAX development kit (Figure 14) that can be used to develop solutions according to both 802.16d and 802.16e standards. It consists of a PCI-X plug-in card (Accelera 3000) containing Aspex's Linedancer processors [28], reference software for the 802.16d/e (PHY) Layer, and an integrated MatLab test-bench environment.

Figure 14: Aspex WiMAX Development Kit [28]

The Aspex WiMAX PHY reference code implements all the mandatory features of the IEEE 802.16d/e PHY layer, and also supports optional features such as sub-channelization and multi-antenna options, enabling initial infrastructure deployments [28]. The reference code runs under Linedancer Extreme Processor which is a fully software programmable, ultra-high performance processor that implements the Aspex ASP architecture.

Despite of implementing all the mandatory features for the PHY layer of WiMAX, this development kit doesn't have a radio board or any code for the MAC Layer. There is also a lack of information about most of the aspects that are considered relevant in this market study.

4.2.2. FUJITSU WiMAX Reference Kit

Fujitsu Microelectronics [29] company provides a WiMAX Reference Kit (Figure 15) that uses the MB87M3550 *System-on-Chip* (SoC) [30], from the same manufacturer, implementing the PHY and MAC layers according to the IEEE 802.16d standard. 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).

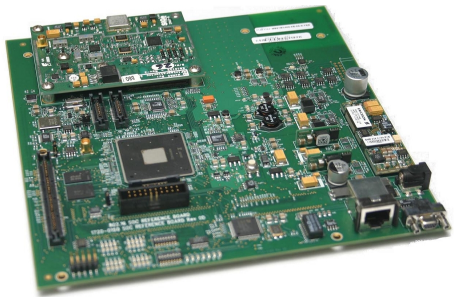

Figure 15: Fujitsu WiMAX Reference Kit

The MB87M3550 SoC has three embedded processors that execute all the PHY and MAC functions: (1) a baseband processor that executes all the OFDM PHY functions (software provided by Fujitsu in binary code), (2) an ARC processor that implements all the lower MAC functions such as CRC calculation and encryption of data (firmware provided by Fujitsu) and (3) an ARM processor that performs all the upper MAC functions (source-code provided by Fujitsu per extra charge). Therefore, this SoC only allows the development of the upper MAC layer functions. It also includes some integrated peripherals like UART/RS-232 interface, I^2C interface, SPI interface, a radio interface and two independent debug ports (ARM and ARC). The development kit includes a radio module that interfaces with the SoC (3.4 – 3.5 GHz), a network and RS-232 interfaces and on-board memory (RAM and Flash). The upper MAC functions run under VxWorks real-time operating system and the development tool is the Tornado IDE from WindRiver.

The development platform from this manufacturer seems to have the necessary requirements to this project 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. The main disadvantage is the high royalty feeds of the RTOS VxWorks and tools associated.

4.2.3. INTEL WiMAX System-on-Chips's

Intel [31] company provides two different SoC's to develop WiMAX solutions: *Intel WiMAX Connection 2250* [32] and *Intel PRO/Wireless 5116 BroadBand Interface* [32]. 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 while the second one only supports fixed WiMAX solutions.

The *Intel WiMAX Connection 2250* is compliant with both IEEE 802.16-2004 and IEEE 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, 802.16 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, i.e., 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 (specially *WiMAX Connection 2250*) but the lack of information about a development kit that implements the SoC necessary hardware is a serious limitation.

4.2.4. SEQUANS WiMAX Development Boards

Sequans Communications [33] company provides two different development boards () that can be used to build SS and BS solutions, respectively, using SoC's from this same manufacturer. The SQN1010-RD [34] board (SQ1010 SoC) can be used to develop SS solutions while the SQN2010-RD [34] (SQN2010 SoC) board is targeted to BS solutions.

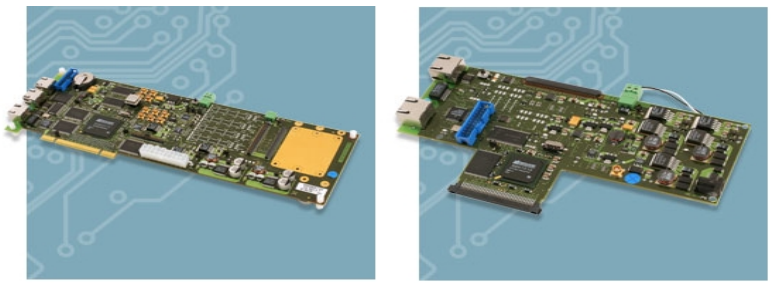

Figure 16: SQN1010-RD and SQN2010-RD development boards [33]

The two SoC above mentioned are quite similar, they both implement all the mandatory functions of the OFDM PHY and MAC layers 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 802.16, PHS, ARQ, privacy (DES and AES) 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 System on Chip's (SoC) and full software package. These two boards are certified by WiMAX Forum (November 2007) and can work in two different modes: RF mode using third party RF module or 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. However, one of the drawbacks presented is the necessity to use different SoC's to implement SS or BS solutions.

4.2.5. TELECIS WiMAX Development Board

TeleCIS Wireless [35] company provides the TCW 1620 SoC and a development board that allows the implementation of fixed/portable WiMAX solutions.

The TCW 1620 SoC [35] 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, 802.16 QoS, ARQ, PHS and AES / DES security and PHY characteristics like uplink sub channelization and 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 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.

4.2.6. WAVESAT WiMAX Development Solutions

WaveSat [36] company has a set of products that can be used to develop WiMAX solutions: an ASIC (*Application Specific Integrated Circuit*) that implements the PHY layer, a MAC Coprocessor that performs lower level MAC functionalities and MAC software running on a specific processor. Using the products described, WaveSat created several development boards that can be used to speed up WiMAX solutions construction.

The Evolutive DM256 ASIC [36] implements the IEEE 802.16d OFDM PHY and is compatible with the IEEE 802.16e. 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 Co processor [36] 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 HCS calculation, encryption, etc.). It is also provided software (source-code) for a WiMAX SS MAC layer tested with 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.

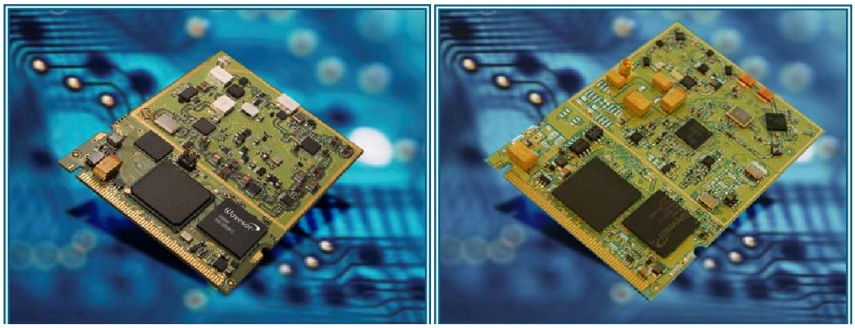

Figure 17: Wavesat Development boards[36]

The solutions from this manufacturer have to be considered because they present good characteristics taking in account 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.

4.3. WiMAX Development Tools Comparison

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 in this project. This comparison can be seen in Table 1 and it is followed by the development platform choice justification.

Table 1: WiMAX development kits comparison

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 Lower MAC and Processor with Upper MAC
Development Board	YES	YES	NO	YES	YES	YES
Standard Compatibility	802.16d and 802.16e	802.16d	802.16d and 802.16e	802.16d	802.16d	802.16d
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

Observing Table 1 it is possible to see that the INTEL company doesn't provide a development board which is an insurmountable drawback because there isn't enough resources to develop all the necessary hardware in the WiRIA project and therefore this manufacturer products will not be considered in this project. All other companies provide development platforms that can be used to speed up a final solution. However, ASPEX company development board will be discarded because it doesn't implement any MAC layer functions nor any base to develop them, which is a serious drawback also due to project resource limitation. The other development boards implement all the mandatory functions of the PHY and MAC layers but, despite of that, only FUJITSU and WAVESATE will be considered because their solutions implement the RF stage, which was a major requirement in the study because there isn't know-how in the WiRIA to project RF circuits.

So, the only companies that provide products that fulfil the requirements for this project were FUJITSU and WAVESAT and therefore one of them was chosen. The development platform chosen was Fujitsu'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 which is the one that we have available in this project.

4.4. Operability with the AN100-U RedLine BS

To assess the WiMAX SS developed in the WiRIA to be used in vehicular applications it is necessary to have a BS that can communicate with it. In this way, the BS chosen was the AN100-U from RedLine communication company which is a certified WiMAX Forum product. As mentioned in the previous section, the solution provided by FUJITSU was already tested with this BS giving the assurance that all the WiMAX main processes are implemented as stated in the standard.

4.5. Conclusions

This chapter presented the study carried out to choose the most adequate development solution to build a WiMAX SS operable with a certified commercial BS. This study started with the definition of the features that were considered of major importance and then all the development solutions studied were presented taking in account the specified features. Next, a comparison among all of them was done allowing concluding that the development tools provided by ASPEX, INTEL, SEQUANS and TELECIS couldn't be used because they did not respect the basic set of functionalities required in this project. The solutions that presented characteristics to be used were FUJISU and WAVESAT ones. The choice made was FUJITSU's because the operability with the Redline commercial BS was already tested and because it presented a much more integrated solution.

Chapter 5

FUJITSU WiMAX Development Kit

This chapter provides a detailed description of the FUJITSU WiMAX Development Kit used to develop a WiMAX SS compatible with a commercial WiMAX BS. In this way, its hardware architecture is first described followed by an overview of the software architecture provided by FUJITSU. An explanation of each software functional block running on each processor present in the hardware architecture is then given focusing all the relevant aspects from the one that is managed by the real-time operating system VxWorks.

5.1. Hardware Architecture

To better understand the structure of the FUJITSU WiMAX Development Kit chosen, an overview of its hardware is presented next. Figure 18 depicts the MB87M3550 SoC and the hardware that interfaces with it. This is the hardware that will be used to develop the WiRIA WiMAX SS.

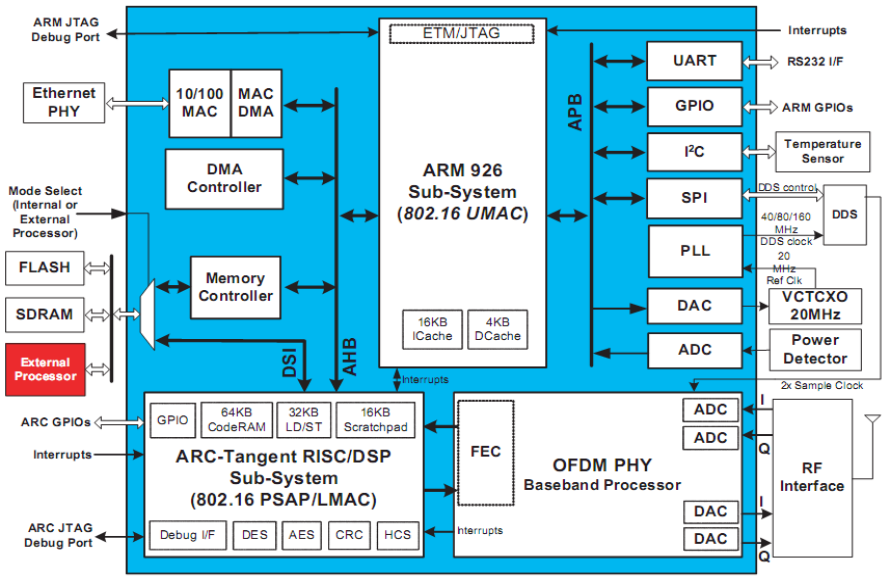

Figure 18: Fujitsu hardware structure [39]

The key features from the MB87M3550 SoC and associated hardware are briefly described in the following subsections. It is also provided an explanation about the interaction among the different hardware blocks (Sub-Systems) depicted in Figure 18.

5.1.1. Integrated ARM926 Sub-System

The ARM926 Sub-System consists in an ARM RISC processor that executes the 802.16 UMAC, implementing the upper level 802.16 MAC functions along with the operating system, protocol stacks, and applications. The ARM926 Sub-System also controls the array of peripherals such as SPI, IIC, etc. as well as the RF circuits. It receives and transmits data by communicating with the PSAP/LMAC running on the on-board ARC-Tangent Sub-System through the shared memories, Code RAM, and LD/ST RAM. The ARM Sub-System is also responsible for downloading the ARC's instruction code into the Code RAM of ARC during the system initialization.

5.1.2. Integrated ARC-Tangent Sub-System

The ARC-Tangent Sub-System consists in an ARC RISC processor that will execute the PSAP/LMAC firmware, implementing lower layer 802.16 MAC functions being the PHY service access point for the UMAC. It can be seen as a bridge between the ARM926 Sub-System (upper MAC functions) and the PHY layer implemented in the Baseband processor. In the transmission, it receives data from the ARM Sub-System and delivers it to the Baseband processor after doing the lower MAC processing. In the reception, it performs the reverse process receiving data from the

Baseband processor and delivering it to the ARM Sub-System after doing the LMAC processing.

5.1.3. Integrated Baseband processor

The Baseband processor implements the PHY transmission chain performing all the mandatory processes from the OFDM PHY. It interfaces with the ARC Sub-System in the way described in the previous subsection, and with the RF board (external to the SoC). When transmitting, it receives data from the ARC Sub-System, performs the PHY functions and delivers an analogue signal to the RF board. In the reception path, it receives an analogue IQ signal from the RF board and delivers digital information to the ARC Sub-System after performing the OFDM PHY processing.

5.1.4. Integrated Peripherals

The main peripherals present in this SoC are an UART/RS-232 interface, I2C interface, SPI interface, memory controller and GPIO's for controlling other peripherals, such as the RF section. These peripherals are used to communicate with SoC external devices for several purposes such as debugging (two independent debug ports for ARM & ARC RISC processors), memory communication (SDRAM and flash), communication over the air for users traffic (RF board), wired communication for users traffic and management (Ethernet PHY and serial using RS-232 protocol).

5.2. Software Architecture

The software provided by FUJITSU with this development kit is adapted to the hardware described above and already implements the processes needed to connect itself with the AN-100U certified WiMAX Redline BS, using a well defined set of WiMAX configuration parameters. This overall FUJITSU software architecture is depicted in Figure 19. As stated in the previous section and observing Figure 19, it is possible to see that the FUJITSU SoC runs three different pieces of software: (1) PHY functions in the Baseband processor, (2) Lower MAC functions in the ARC processor and, (3) the upper MAC functions, protocol stack, applications and operating system in the ARM processor. The PHY block and LMAC software are provided in binary code by FUJITSU and therefore it is not possible to change any of its features. The only software that can be partially changed is the one that is running on the ARM processor and it will be mainly focused next. The different software functional blocks that are executed on the ARM processor are explained in the next subsections (Figure 19).

5.2.1. RTOS (Operating System)

Many of the tasks created in the ARM processor exhibit real-time requirements (for example

latency), thus a RTOS was used, VxWorks in the case, to achieve tasks execution predictability. VxWorks 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 to run. For tasks having the same priority it is possible to enable a round-robin algorithm that aims at sharing the CPU among tasks with the same priority.

The RTOS wrapper is an abstraction layer providing a uniform operating system interface to the upper layers. With the help of this layer, RTOS dependencies of the upper layers are minimized. If porting to a different RTOS is desired, most porting efforts would be directed to this layer, rather than the other software components [39]. Related to the RTOS block, there is an API layer that provides some of the RTOS resources to be used by other software blocks.

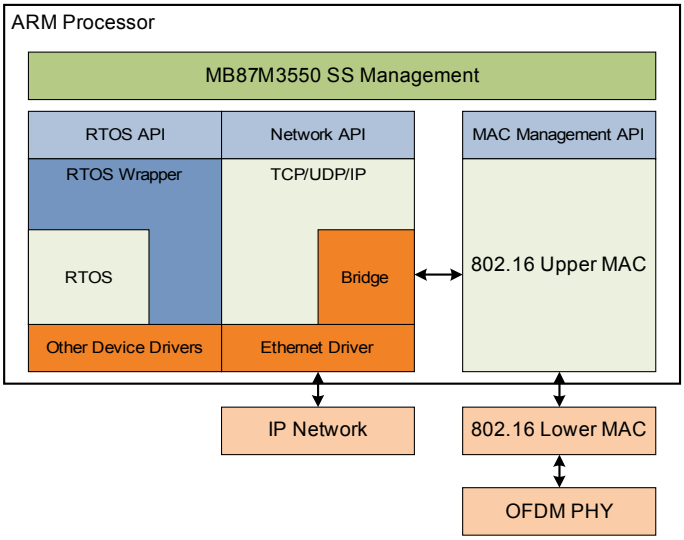

Figure 19: SoC Software Architecture [39]

5.2.2. MB87M3550 SS Management

The MB87M3550 SS Management Module is an application layer software component responsible for managing the high-level SS functionalities. The functions of this module include system initialization, configuration file management, software upgrades, and user interfaces for local management and configuration functions. This is the foremost component with which the end user interacts and that uses the API layers provided by the RTOS, Network and MAC Management. This software is provided by FUJITSU in source-code allowing the user to change it.

5.2.3. TCP/UDP/IP Protocol Stacks

The TCP/UDP/IP stack contains the network protocols TCP, UDP, and IP, organized as a closely

coupled protocol suite, along with a library of some other useful protocols. The services provided by TCP/UDP/IP protocol stack are accessible to other modules through the Network API. This protocol stack is provided by Wind River along with the RTOS VxWorks.

5.2.4. 802.16 UMAC Protocol Stack

The 802.16 UMAC is a software implementation of 802.16 MAC as defined in IEEE 802.16-2004. The UMAC provides higher level 802.16 MAC functionality, MAC management layer, service specific convergence sublayer, common part sublayer, privacy and authentication, and key management services. FUJITSU provides a MAC management API layer to perform some configuration and monitoring to UMAC processes. This software provides the connectivity with the AN-100U Redline BS using a defined set of configuration parameters. Specifically, the connectivity is only achieved using a frame duration of 10 ms and a cycle prefix length of 1/16. It is important to say that only BE and rtPS service classes can be used because Redline BS does not support the other ones. This software block is provided in binary code and cannot be changed.

5.2.5. Bridge

The FUJITSU SS-UMAC is attached to a link-layer packet bridge directing Ethernet packets destined for 802.16 stack to 802.16 MAC service specific convergence sublayer and vice-versa. This module is provided by FUJITSU in source-code. This block performs an analysis on the destination of incoming data delivering it to the correct block (802.16 UMAC, Ethernet Driver or Network Stack). The specific work performed in this block is explained ahead.

5.2.6. Device Drivers

The Ethernet Driver is the software device driver for the 10/100 Ethernet MAC in the MB87M3550. It is responsible for handling interrupts generated by the Ethernet MAC and transferring data in and out of it. There are device drivers required and used by other system software components such as SPI, IIC and UART drivers, etc. The Ethernet Driver is provided in source-code by FUJISTU but all the other are not.

5.3. FUJITSU Tasks Description

The software functional blocks described in the previous section are running in the ARM processor and their execution is managed by the VxWorks RTOS. In this way, all the work performed in this processor is done under VxWorks tasks according to the scheduling algorithm of this RTOS. All the tasks that execute the software blocks above mentioned are described and explained next.

5.3.1. VxWorks System Tasks

The RTOS VxWorks provides not only all the properties of a real-time operating system but also some optional components and services that can be used to improve the overall behaviour of the system and facilitate the interaction with it. Depending on its configuration, the VxWorks system can include a variety of system tasks. Those used in FUJITSU software are described in Table 2.

Table 2: Fujitsu Software: VxWorks System Tasks

Task name	Priority	Description
tExcTask	0	This task supports the VxWorks exception handling package by performing functions that cannot occur at interrupt level.
tLogTask	0	This task is used by VxWorks modules to log system messages without having to perform I/O in the current task context
tWdbTask	3	This task is used to answer to requests from the the Tornado target Server (running on the host) to perform system analysis.
tNetTask	50	This task handles the task-level functions required by the VxWorks Network.
tFtpdTask	55	This task handles the FTP client requests spawning new tasks for each connection that is set up. It implements an FTP server.
tTffsPTask	100	This task handles all the processes needed to implement and manage the flash memory file system.
tDcacheUpd	250	This task optimize disk access, reducing the number of times the disk head needs to move when mechanical hard disks are involved.

The tasks described in Table 2 implement functionalities provided by VxWorks and therefore it is not possible to know which code is executed by each task (binary code). The choice of including a certain functionality is done using Wind River menu provided with the Integrated Development Environment TORNADO.

5.3.2. UMAC Tasks

The UMAC software block is provided by FUJITSU and implements all the mechanisms needed to connect to the Redline BS. This software is not provided in source-code so it is not possible to know which is the execution path of each task created. However, VxWorks provides a way of observing the tasks that are running on the system. The tasks created in the UMAC software are described in Table 3.

As stated before, these tasks run the software from the 802.16 UMAC block to establish and manage a connection with Redline BS handling all the data to/from it. Besides that, some of the work done in the MAC Bridge and in the Ethernet Driver is also performed by a UMAC task using a call back function. These processes will be described in the following section.

Table 3: Fujitsu Software: UMAC Tasks

Task name	Priority
tMacTx	5
tMacCps	10
RxTask	12
tMacCs	25
tMacDlCps	30
tMacLog	50

5.3.3. User Application Task

The software provided by FUJITSU includes a module (MB87M3550 SS Management) that consists in a user interface (menus) accessible through the RS-232 interface and that makes possible to a user to perform some configuration and monitoring using the API layers from the RTOS, Network and UMAC. There is only one task that performs this work and it is described in Table 4.

Table 4: Fujitsu Software: User Application Task

Task name	Priority	Description
App Task	40	This task is responsible for executing the user interface software (menus provided by FUJITSU) and to handle the users configuration and monitoring.

All the code executed by this task is provided in source-code by FUJITSU and therefore it is possible to perform analysis and modifications.

5.4. Communication Tasks Analysis

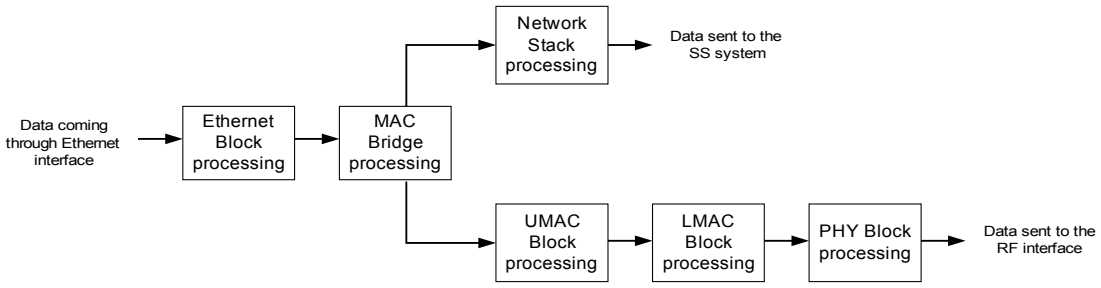

Figure 20: Ethernet Data: processing order

After describing all the tasks that run the software provided by FUJITSU, it is important to understand which tasks are involved when the SS is communicating with external devices such as a WiMAX BS (RF interface) or an IP Network (Ethernet interface) either in the incoming and outcoming direction. It is also necessary to understand which is the software code that each task executes when receiving / sending data through these two main interfaces.

When data is coming from the Ethernet interface, it enters directly to the ARM processor through the Ethernet block that makes it accessible in a shared structure for the MAC Bridge. Then, this data is sent to the SS system or/and to the UMAC block to be sent over the air (Figure 20). On other hand, when data is coming from the RF interface, it should be first processed by the software that executes on the Baseband and ARC processor and then enters the ARM processor to the UMAC block. This block make this data accessible to the MAC Bridge that then sends it to the Ethernet Block (to be sent through the Ethernet interface) or/and to the SS system (Figure 21).

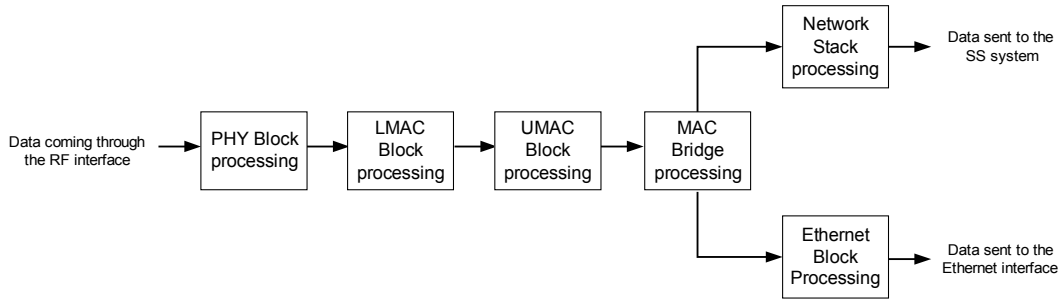

Figure 21: RF Data: processing order

5.4.1. Ethernet Data

When a packet enters the ARM processor through the Ethernet interface, an interrupt is generated. At the interrupt level, the packet is copied to a shared structure and a new job is added to the VxWorks task *tNetTask* passing as an argument the Bridge routine that will be executed at this task level. In this Bridge routine the packet destination address is inspected. If the destination packet is the SS itself then it is delivered to the SS network stack calling a specific VxWorks routine after doing some required processing. However, if the packet destination wasn't the SS, then the Bridge routine checks if the packet is broadcast. If so, the packet is copied and sent either to the network stack and to the UMAC (calling respective routines) after performing some specific processing in the first case. If the packet is neither broadcast nor destined to the SS then a UMAC routine is invoked at the *tNetTask* level to transmit the packet over the air. This process is depicted in Figure 22.

5.4.2. UMAC Data

When data is entering through the RF interface, it is first processed by the software running on the Baseband and ARC processor before entering the ARM processor. In the ARM processor this data is collected by a UMAC task and all the UMAC processes are executed under the UMAC tasks described in Table 3. When leaving the UMAC block, the packet processing is done at the

tMacDlCps level calling a call back function. At this level, a routine from the bridge is called in order to inspect the packet destination. If the packet is broadcast then it is copied, processed and delivered either to the network stack and Ethernet calling the respective routines. If the packet destination is the SS itself then the packet is processed and delivered only to the network stack. However, if the packet destination is neither the two previous addresses then it is delivered to the Ethernet Driver. This process is depicted in Figure 23.

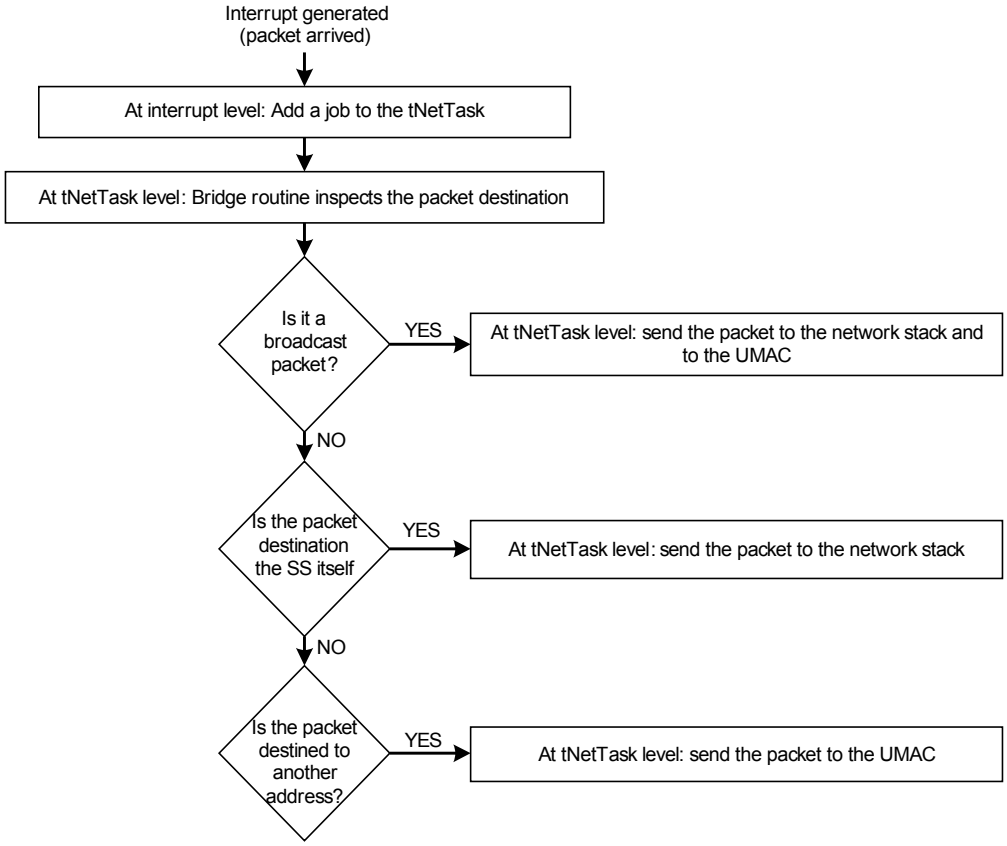

Figure 22: Ethernet Packet Processing

5.4.3. System Network Stack Data

If the SS Network Stack needs to send a packet to external entities then it can only deliver this data to the Ethernet Driver not being able to send it to the Bridge to be inspected. In this way, it is not possible to send packets from the SS Network Stack to the RF interface. All the work done when sending packets from the Network Stack to the Ethernet Driver is performed under *tNetTask level*.

5.5. Conclusions

This chapter has described the hardware and software architecture provided by the FUJITSU Development Kit that will be used to develop a WiMAX SS fully operable. Despite of

implementing several mechanisms needed to implement a WiMAX SS that were useful, it was necessary to correct, improve and add some processes to transform this development kit in a real WiMAX SS solution that could be easily used and managed by a common user. The work done to create this WiMAX SS solution is explained in the next chapter.

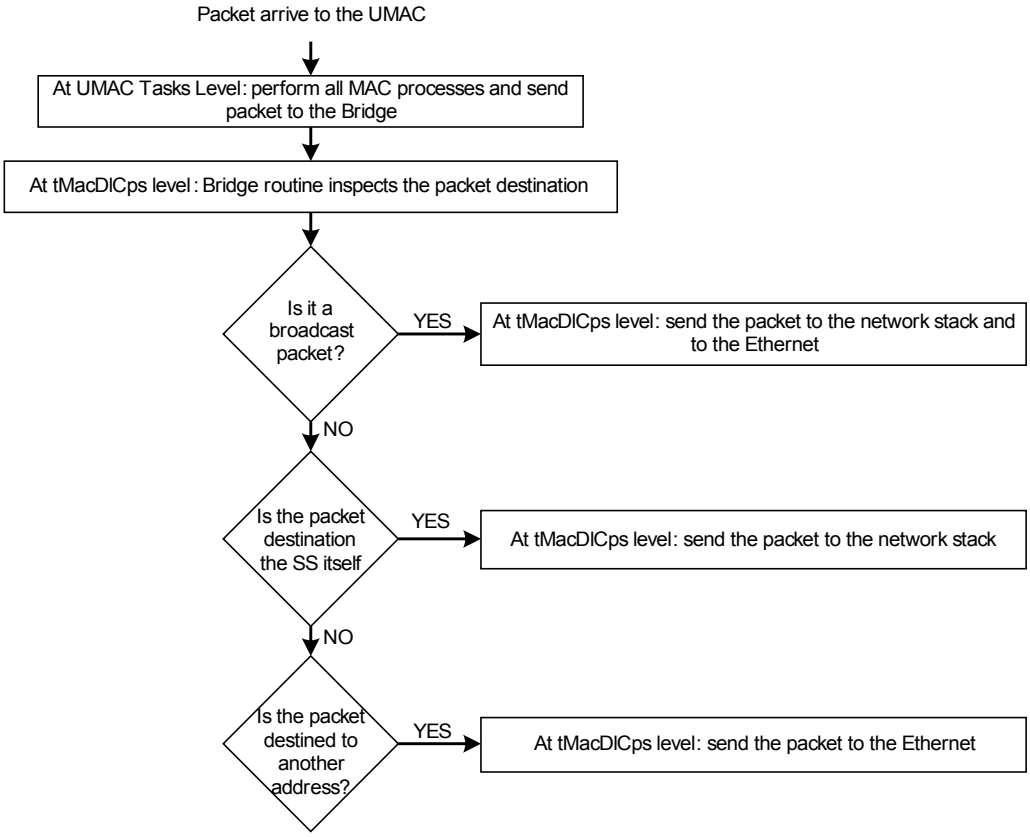

Figure 23: UMAC Packet Processing

Chapter 6

WiMAX SS Architecture

As stated in the previous chapter, the FUJITSU Development Kit hardware and software were used to build a WiMAX SS fully interoperable with a certified Redline WiMAX BS. However, this development kit doesn't provide the functional nor management necessary features to be used in a V2I communication scenario and, therefore, some new functionalities were added and some existing software was changed with the purpose of adapting the WiMAX SS to be used as a vehicular communication OBU, always taking in account the objectives of the WiRIA project.

6.1. SS Software Architecture

The software provided was partially changed to add new functionalities needed creating, in this way, a new software architecture (Figure 24). Some of the software blocks were used as provided by FUJITSU, other were changed and new blocks were implemented (in the ARM processor).

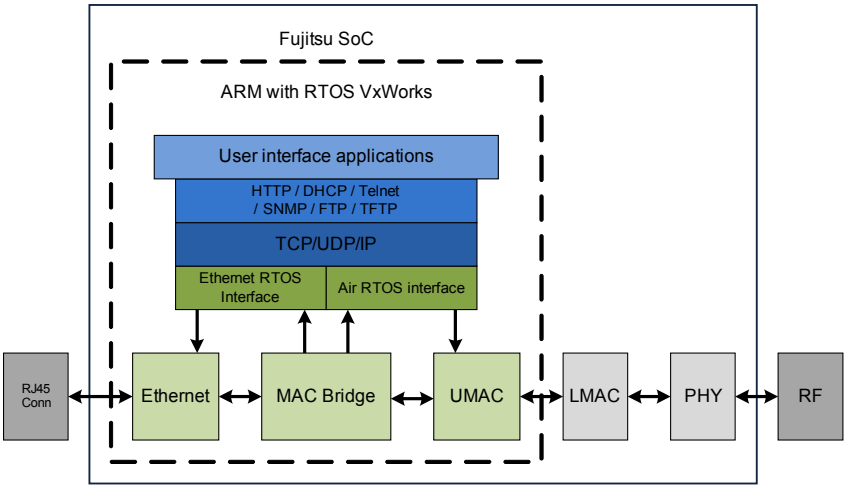

Figure 24: WiRIA SS Software Architecture

It is possible to see that the data can enter the SoC either by the RF interface (air) or the Ethernet interface (RJ-45 connector). If it enters through the RF interface then it has to be first processed by the PHY block and Lower MAC software before entering the ARM processor which execution is partially controlled. On the other hand, if the data enters through the Ethernet interface it can be collected directly to the ARM processor (Ethernet block).

6.1.1. SS Software Changes Overview

In Figure 24, the RTOS block is not explicitly shown but it is used to perform the tasks execution management. The UMAC block is here used exactly as provided by FUJITSU since it provides the connectivity with the Redline BS and it is impossible to change any of its features. The Ethernet block is also used as provided initially because it implements all the functionalities needed to handle packets coming from the Ethernet interface. The MAC Bridge software block was changed to allow the SS system to communicate with both interfaces: RF and Ethernet. To perform that, it is also necessary to add a new device to the network stack (Air RTOS interface). The user interface module provided by FUJITSU was removed and instead some new ones were developed being accessible using network protocols that were also implemented. A detailed description of each block mentioned is provided next.

6.2. SS Developed Software

Looking at the software architecture provided by FUJITSU (Figure 19, Chapter 5) it is possible to identify some problems from a vehicular communication perspective: the SS system is not able to send information to the UMAC block and therefore, the communication with the SS (OBU) system

from the air interface is impossible to achieve (all generated SS system packets are always sent to the Ethernet interface). Other problem found is that the management interface provided can only be accessed locally using the RS-232 interface, creating then limitations for the infrastructure to manage the OBU, if necessary. In this way, the solutions developed for the problems mentioned above are described next.

6.2.1. SS System to RF interface Communication

Due to the first problem mentioned above, in a V2I scenario using FUJITSU software, the infrastructure (RSU) was unable to communicate with the OBU internal system using the RF interface. So, if the OBU (WiMAX SS) was integrated in the vehicle ECU it would be impossible to communicate with the RSU (WiMAX BS) to provide any safety related information or other. This situation was less problematic if the WiMAX SS was a stand-alone part that communicates with the ECU using an interface (for example Ethernet) because, in this case, the ECU could communicate with the RSU to send safety information. However, the OBU system would be still inaccessible from the air interface for management and update processes anyway. To solve this problem, the Air RTOS interface block was added and the MAC Bridge software was changed.

The Air RTOS interface is the block that the SS network stack (TCP/UDP/IP) sees when trying to communicate with the UMAC block. This block is similar to the Ethernet RTOS interface but calls a specific call back function from the MAC Bridge when the packets' destination is the RF interface. Therefore, it is responsible for accepting data packets (which destination is the UMAC) from the network stack and to deliver this information to a specific MAC Bridge routine. In this way, it is now possible to communicate with the SS system using both RF and Ethernet interfaces.

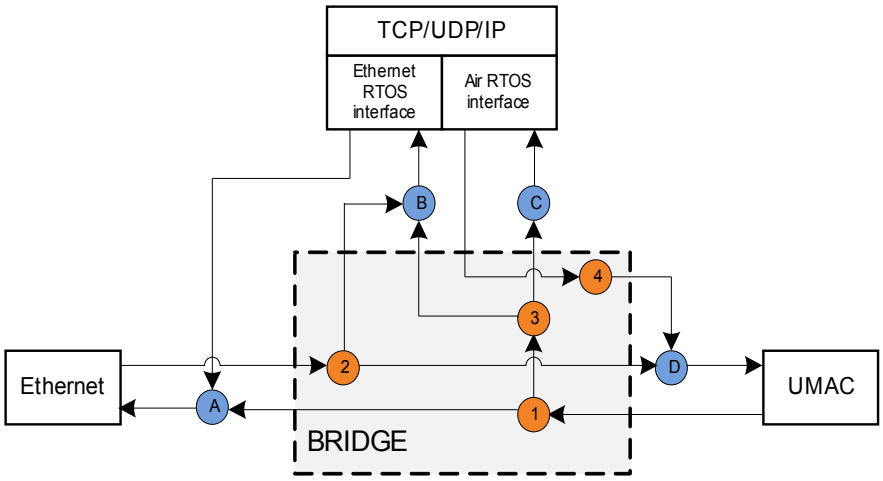

Figure 25: MAC Bridge Architecture

However, there were still some problems when trying to communicate with both interfaces due to an issue from the TCP/UDP/IP system network stack that doesn't allow to bind a specific IP port

(for example port 80 for HTTP) to more that one device, two in this case: Ethernet RTOS interface and Air RTOS interface. Therefore, it was impossible to communicate, using the same application layer protocol, with the SS system using both the RF and Ethernet interfaces. Based on Figure 25, it is provided an explanation about the solution developed to solve this problem. This figure shows the MAC Bridge architecture and the blocks that interface with it. The main purpose of the MAC Bridge is to inspect the packets destination, perform some specific processing when needed and deliver each packet to the correct receiver block.

The process done when a data packet is sent to the MAC Bridge by the Ethernet block remains the same: the first task performed is the destination address inspection (point 2) and depending on it, the packet is delivered to the reception point of the Ethernet RTOS and/or UMAC (point B and/or D).

However, due to the problem above referred, some new processing must be done when the UMAC sends a data packet to the MAC Bridge: the packet destination address is first inspected (point 1). If the destination is the Ethernet block then it is only necessary to deliver it to the reception point of Ethernet (point A). However, if the packet is for the SS Network stack, then it is necessary to perform some processing (point 3) that consists in checking if the packet is from some TCP or UDP application (related to the TCP/UDP/IP issue mentioned before). If so, the packet IP and MAC destination addresses are changed to the IP and MAC addresses from the Ethernet device and the new checksums are calculated. After this, the packet is delivered to the Ethernet RTOS interface reception point (point B). However, if the packet is not from a TCP or UDP application then it is delivered to the Air RTOS interface reception point (point C) without performing any change. The processing done when the packets belong to a TCP/UDP application means that from the SS network stack point of view, the packet has been sent from the Ethernet interface.

When the SS network stack delivers packets, the processing done depends on their destination address. If a packet destination address belongs to the Ethernet interface network then the packet is sent to the Ethernet RTOS interface and then it is delivered directly to the Ethernet reception point (point A). However, when the packet destination is an address belonging to the Air interface network, the Air RTOS interface is responsible to send the packet to the UMAC after performing some necessary processing (point 4). This processing consists in checking if the packet belongs to a TCP/UDP application and if so, changing the source IP and MAC addresses to the Air interface IP address, delivering it to the UMAC reception point (point D).

6.2.2. User Applications and Network Protocols

The other blocks depicted in Figure 24 are network stacks (TCP/UDP/IP, Telnet, DHCP, FTP, TFTP, HTTP and SNMP). These protocols were used to develop applications for user interfaces purposes to provide an easier way of SS management through the implementation of a Website, Remote management using XML files, CLI and SNMP traps, etc.

Some of the protocol stacks mentioned above were provided along with the RTOS VxWorks (TCP/ UDP/IP, Telnet, DHCP, FTP and TFTP) implementing functionalities needed to develop some users applications described next. The HTTP network protocol implementation was acquired from the GoAhead Software company [40] and already implements a web server that handles all the HTTP protocol processes. The construction of SNMP traps was also added to allow the SS to spontaneously inform an external entity about the occurrence of SS specific internal events (it is not an SNMP agent) without having to wait for requests.

Using the network protocols mentioned above, some user interface applications were developed to facilitate the SS remote management. The user interfaces developed are related not only with the adaptation of the WiMAX SS to be used as an OBU but also with the objectives of the WiRIA project. In this way, a website was created, using the HTTP protocol, to allow users to manage all the SS parameters either through the Ethernet or RF interfaces by using a common web browser. These parameters are not only related with RF, PHY and MAC SS features but also with operability (DHCP for acquiring IP dynamic address) and update issues (using FTP or TFTP). These parameters are also manageable using a CLI that can be accessed locally via RS-232 interface or remotely using the Telnet Protocol. Another way of remotely managing all these SS parameters is using XML files in HTTP message. This process consists in transporting XML files in HTTP messages to perform configuration and monitoring. In the configuration case, an HTTP Request message can be sent to a specific SS URI transporting a well formatted XML file with the parameters and values to be configured. In the monitoring case, an HTTP Request message should be first sent to a specific SS URI and then the SS responds with an HTTP Response message containing a well formatted XML file with the parameters and associated values requested. In the first case, an XML Parser was developed to perform the interpretation of the configuration XML file received by the SS. Last, an alarm system was also developed using SNMP Traps, so whenever a specific event occurs in the SS, an SNMP trap is generated and sent to a configured IP address to inform about the event occurrence.

6.3. SS System Communication

After describing the changes made to allow the BS (RSU) to communicate with the SS (OBU) system, it is important to understand the overall processing done when the SS system is sending/receiving packets to/ from the RF interface because it is a process that has impact on a V2I communication scenario in terms of delay. The information that is received/sent to the RF interface can be provided to/by SS internal applications (SS system) or external applications running on other system using the Ethernet interface. So, it is also important to know the execution performed when packets are coming through the Ethernet interface.

6.3.1. Air Interface

When a packet enters the SS system through the RF interface, it begins to be processed in the two processors that implement the PHY and LMAC processes entering next in the ARM processor. In this last processor, the packet is sent to the UMAC block which processing is done by specific

UMAC tasks. After this, all the MAC Bridge software is executed at the UMAC *tMacDlCps* task level until sending the packet to the Ethernet or to the SS system using the specific functions provided by either blocks. This process is depicted in Figure 26.

On the other hand, when a packet is sent from the SS system to the RF interface, it is necessary to execute some MAC Bridge software before sending the packet to the UMAC block. This processing is done at the VxWorks System *tNetTask* level until delivering the packet to the UMAC using the specific provided function. After this, the packet will be processed by the LMAC and PHY processors before being sent through the air. This process is shown in Figure 27.

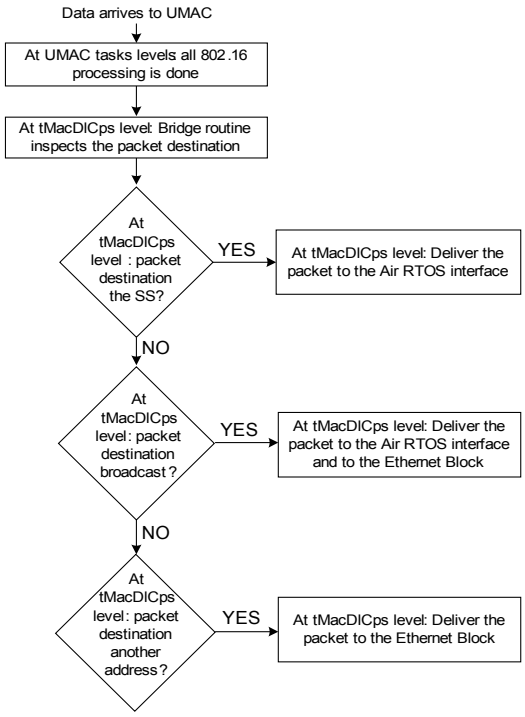

Figure 26: Air interface: UMAC data

The processes described in Figure 26 and Figure 27 show all the processing done to the data packets when there is communication among the SS system and the RF interface and vice-versa. The VxWorks tasks that perform the execution on the ARM processor are described ahead.

6.3.2. Ethernet Interface

For each packet entering the Ethernet interface, an interrupt is generated to the ARM processor, and, at this level, the incoming packet is placed in a shared memory pool and a message is sent to the *tEthRcvQ* to wake it up and execute processing on the incoming packet. So, all the execution from the MAC Bridge is performed at the *tEthRcvQ* level until delivering the packet to the SS system or to the UMAC calling the specific provided functions (Figure 28).

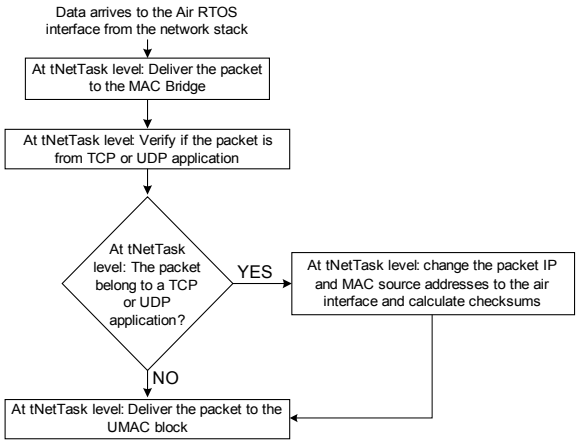

Figure 27: Air interface: SS system data to UMAC

6.4. System Tasks Description

To execute the software previously described under RTOS VxWorks, several tasks were created, associating a priority to each based on their importance in the system. So, this section provides a description of the tasks that implement each software block described in Figure 24. Some of them remain the same from the FUJITSU software and therefore they will be only referred but not explained in following subsections. It is important to refer that some work is also executed at the interrupt level and that consume processing time.

6.4.1. UMAC Tasks

The UMAC tasks (see Table 3, Chapter 5) that execute the UMAC software block and handle the packet entry and exit through the UMAC-LMAC interface remain the same from the FUJITSU software not only because it is impossible to change them (created in closed software) but also because they execute all the necessary work to achieve a satisfactory communication with the Redline BS.

6.4.2. VxWorks System Tasks

The tasks from the VxWorks System used in this SS system are different when comparing with the software provided by FUJITSU (see Table 2, Chapter 5). Some of the tasks remain the same but others were removed. The tasks that remain the same are *tExcTask*, *tLogTask*, *tNetTask*, *tTffsPTask* and *tDcacheUpd* because their work implement functionalities needed by the SS system. On the other hand, the tasks *tWdbTask* (that managed the communication with the host for analysis and

debugging purposes) and *tFtpdTask* (that implemented an FTP server) were removed because they implement functionalities that were considered not necessary neither from a V2I communication perspective nor considering the WiRIA project objectives.

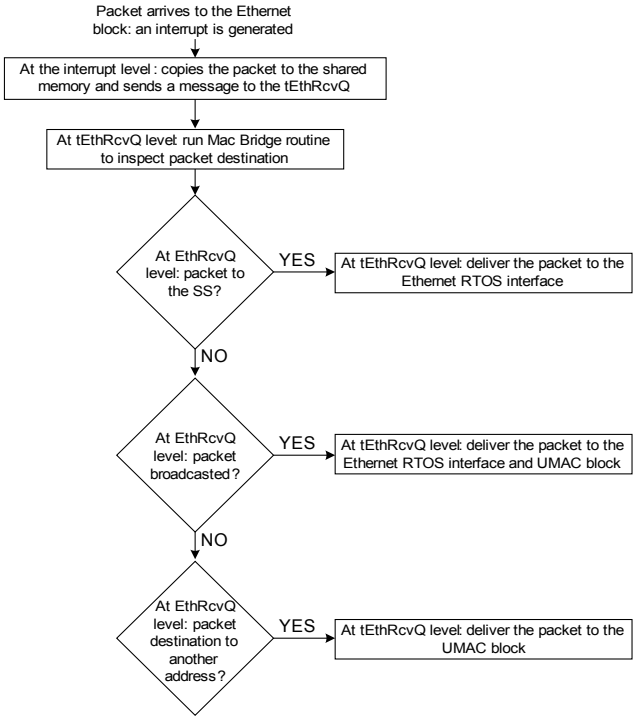

Figure 28: Ethernet interface: Data entering the Ethernet

6.4.3. Network Stacks Tasks

Table 5: WiMAX SS VxWorks System Tasks

Task Name	Priority	Description
tTelnetd	55	Telnet daemon. It accepts a remote login request from another VxWorks or host system and spawns the input task *tTelnetInTask* and output task *tTelnetOutTask*.
tDhcpReadT	56	This task along with other VxWorks tasks handles the DHCP traffic and all the low-level processes needed to acquire a dynamic IP address.
tDhcpState	56	This task along with other tasks handles the DHCP traffic and all the low-level processes needed to acquire a dynamic IP address.
tAirDhcp	101	This task manages a state machine needed by the DHCP protocol to control the acquisition and renewal of the dynamic IP address.

These tasks execute work needed by the DHCP and Telnet Protocol. The *tTelnetd* task performs all the required processing to accept a remote request from the host and to manage all the communication with it. The *tDhcpReadT* and *tDhcpState* tasks handle all the DHCP processes needed to acquire a dynamic IP address. The creation of the *tAirDhcp* task is required in order to control the acquiring and renewal times of the IP dynamic address using a state machine. These tasks are summarized in Table 5.

6.4.4. Ethernet Tasks

The *tEthRcvQ* task does the work that the *tNetTask* was performing in the FUJITSU software when receiving packets from the Ethernet. That is, instead of adding a job to the *tNetTask* at the interrupt level when a packet is received from the Ethernet interface, a message is sent to the *tEthRcvQ* task to wake it up and run all the software from the MAC Bridge until deliver the packet to the correct reception point.

Table 6: WiMAX SS Ethernet Task

Task Name	Priority	Description
tEthRcvQ	49	This task handles all the processing performed in the bridge when a data packet is received through the Ethernet interface.

This task was added with the purpose of creating a separation between the traffic that goes directly from Ethernet to UMAC (and vice-versa) and the traffic from both Ethernet and UMAC to the SS system. The traffic among the Ethernet and UMAC is never processed at the *tNetTask* level being processed by: (1) the *tEthRcvQ* task when a packet enters through the Ethernet interface and (2) the *tMacDlCps* task when entering by the UMAC-LMAC interface. However, when the traffic is from/to the SS system, the *tNetTask* always performs some or all the packet processing. That is, even if a problem occurs with the *tNetTask*, the traffic from the Ethernet to the UMAC and vice-versa is still enabled, being possible for an entity that is connected to the Ethernet interface (for example a vehicle ECU) to continue to send traffic (safety traffic) to the air.

6.4.5. MAC Bridge Task

Table 7: WiMAX SS MAC Bridge Task

Task Name	Priority	Description
tMacBrdgMod	40	This task verifies if the UMAC block is enabled or not (causes the MAC bridge to change its behavior accordingly).

The *tMacBrdgMod* task verifies the state of the UMAC block because, depending on it, the behavior

of the MAC Bridge can change. When the UMAC is enabled, the MAC Bridge does the destination address checking to forward the packets to the destination reception points as stated in the MAC Bridge description. However, when the UMAC is disabled, there is no traffic passing to or from the air and therefore the MAC Bridge only verifies if the packets coming from the Ethernet are for the system and vice versa, discarding all the others.

This task avoids the execution of unnecessary work when the UMAC is disabled (there is no traffic passing to or from the air). It is possible, in this way, to decrease the load on the system and then improve its performance.

6.4.6. User Interfaces Tasks

Table 8: Other WiMAX SS Tasks

Task Name	Priority	Main Routine
tSnmpt	103	This task sends SNMP traps when a specific event has occurred in the SS system.
tWebServer	54	This task runs all the processes needed to implement a web server receiving requests from external entities and providing the consequent responses.
tCLI	59	This task runs all the processes needed to implement CLI. This CLI is accessible through the RS-232 interface or remotely using telnet.

The tasks described in Table 8 implement the user interfaces. They implement the web server responsible for managing the web site and the configuration using XML, the CLI that can be accessed remotely using Telnet or locally using RS-232 interface and the alarm system that uses SNMP traps every time a specific event occurs.

6.5. System Tasks Priority Assignment

It is possible to observe that the tasks that execute in the SS system were divided in logical groups in the previous section and that all the tasks have an associated priority. This priority was assigned based on the importance of the work that each performs on the system. So, this section provides an explanation about the priority assigned to the tasks in each logical group mentioned before.

The tasks that belong to the UMAC block are created in the software provided by FUJITSU in binary code. Therefore, it is not possible to fully justify the priority assigned to them. As stated before, these tasks implement all the 802.16 processes needed to handle a WiMAX connection with

the Redline BS. Some of these processes, such as the 802.16 network entry process or the construction of the 802.16 frame (see Chapter 3) to transport information over the air, have timing constrains associated that should be respected in order to assure a correct WiMAX connection behavior. So, the main reason to give the UMAC tasks such high priorities (see Table 3, Chapter 5) is to assure the fulfilment of these constrains and to maintain a satisfactory WiMAX link with the BS.

Other tasks that were created in closed software are the VxWorks System tasks that implement functionalities needed by the RTOS to work properly. The priority assigned to each task was used as defined by RTOS VxWorks (see Table 2, Chapter 5).

The tasks associated with the Network Stack implement processes needed by the Telnet and DHCP protocols and the priority assigned to each task is the default by VxWorks. It is possible to observe that the priority is properly assigned because they implement network protocols that need to use data packets coming from the network interfaces. So, it is required that they have a lower priority than the *tNetTask* and *tEthRcvQ*, that have a priority of 50 and 49, respectively because these two last tasks have a major importance and are more sensitive to delays than the first ones.

As previously mentioned, the work performed by the *tMacBrdgMod* task is very simple and consists in verifying the state of the UMAC. Therefore, this task will be most of the time in the delayed state waking up periodically only to verify the mentioned state. In this way, the priority assigned (40) is higher than the task that handles the packets coming from the Ethernet (*tEthRcvQ*) because the work that this last task performs can change depending on the UMAC state.

The *tEthRcvQ* task performs all the work needed by the packets that enter through the Ethernet interface until be delivered to the UMAC block (then processed by UMAC tasks) or to the SS system (then processed by *tNetTask*). The introduction of this task has the purpose of dividing the traffic which is directed to the SS system from the one which passes directly from the network interfaces. In a V2I perspective, the WiMAX SS can be seen as stand alone part that that uses a communication interface (Ethernet for example) that connects to a ECU so, the traffic among the two network interfaces has a major importance and then the priority assigned to the *tEthRcvQ* was 49, higher that the *tNetTask* (50). This priority was assigned close to the *tNetTask* one to not interfere with other processes that are time critical (UMAC for example).

The tasks from the User Interface block work on packets coming from both interfaces using network protocols implemented in the SS. In this way, they were assigned a lower priority than the tasks that handles the packet entry through both interfaces (*tEthRcvQ*, *tNetTask* and *tMacDlCps*). Inside this block, it is possible to observe that the priority assigned differs depending on the application implemented. The Web server that handles the web site and remote management using XML was considered the most important application user interface because it is the more common and easy way of managing the SS. The *tCLI* task was assigned a lower priority than the *tTelnetd* because this network protocol can be used to access it. The alarm system and the DHCP protocol machine state were assigned a lower priority because they implement functionalities that were not important in this stage.

6.6. Conclusions

This chapter has provided a description of the WiMAX SS software architecture that will be used to study and assess WiMAX for V2I applications from the OBU side. To achieve this, the FUJITSU software main problems were first identified and then the solutions developed to solve them were presented. Those solutions consisted in changing some existing software and to develop new one. Next, the communication performed among the SS main communication interfaces (RF and Ethernet) was focused and last, the task running on the processor (under VxWorks RTOS) were explained and their priority assignment was discussed.

Not all the work performed was targeted to the construction of a WiMAX OBU due to the WiRIA project requirements. The purpose was to use the WiMAX SS developed, giving it all the functionalities needed from a vehicular communication perspective without compromising the WiRIA project objectives in terms of operability and management. In this way, this solution can be improved in terms of vehicular communication but it is a good equipment to start the study of this technology for V2I applications. So, the WiMAX SS developed will play the role of an OBU that communicate with the infrastructure using a RF link with the RSU (Redline Communications BS) sharing road safety information.

Chapter 7

V2I Services Using WiMAX

In the two previous chapters, the SS software architecture used to assess WiMAX for vehicular communications was described. This WiMAX SS can be seen as an OBU that resides on each vehicle on the road. In this way, it is possible to study the supply of V2I services using WiMAX wireless technology. An aspect that is crucial for many application fields, including V2I, is the characterization of the diverse service classes in aspects like bandwidth, latency, timeliness, set-up times, etc. So, this chapter presents the requirements of different V2I services and assesses the suitability of the WiRIA SS and WiMAX QoS service classes to provide such services. To achieve this purpose, some experimental results obtained using the WiRIA and Redline SS's are shown.

7.1. Introduction

Some of the features of the WiMAX technology seem to match the V2I applications requirements,

making this technology a good candidate to serve at the V2I infrastructure level. The set of requirements imposed by the V2I services is heterogeneous, existing services with high bandwidth needs but with no timeliness requirements while others present strict timeliness constrains but are not demanding in terms of bandwidth. In this way, it is possible to assess the possibility to use WiMAX, with its different QoS classes, to properly differentiate these services.

WiMAX provides a bidirectional communication link on a TDD or FDD scheme. In this way, it is possible for the RSU to send safety information or other to the vehicles and for the vehicles OBU's to inform the infrastructure about dangerous road situations perceived using on-vehicles local sensors. Using a TDD scheme, it is also possible to give configurable dedicated transmission times to the downlink (RSU to OBU's) and uplink (OBU's to RSU) directions, improving the bandwidth usage efficiency when there is traffic asymmetry.

Complementary, WiMAX integrates traffic differentiation and bandwidth allocation mechanisms that allow the coexistence of different traffic classes with diverse QoS guarantees. Unsolicited Grant Services (UGS) supports fixed-sized data packets at constant bit rate. Real-Time Polling Service (rtPS) supports the transmission of periodic variable bit-rate traffic. Generic delay-tolerant traffic, e.g. resulting from file transfer is supported by the Non-Real-Time Polling Services (nrtPS). On the other hand, traffic classes that does not require a minimum service-level, e.g. Web browsing, is supported by the Best-Effort Class (BE).

Finally, the large coverage range, that may reach tens of Km, allows reaching broad areas with a minimum number of RSU's, with important consequences in installation and maintenance costs.

In this way, WiMAX traffic differentiation could be used to provide several types of road services taking in account and respecting their different requirements in terms of reliability, bandwidth and timeliness being possible to provide simultaneously road safety information and other types of non-critical safety applications in either downlink and uplink directions.

7.2. V2I Services Characteristics

As stated before in this document, V2I systems should support diverse V2I services with different characteristics. These services were divided in three different categories that can be mapped in WiMAX QoS service classes depending on their specific requirements. These V2I services are described in the following subsections.

7.2.1. Safety Warning / Assisted Driving

In these types of V2I services, the information that is provided to the vehicles have timeliness and reliability requirements and any failure can have a negative impact in terms of road injuries,

fatalities or in economy. In this way, it is necessary that this information is always delivered in time to its receiver in order to maintain its usefulness.

The messages associated with these services are sent by the RSU to inform the drivers of specific events and to help them to take the correct behavior when facing potentially dangerous road situations. The Safety Warning services are used to inform drivers about dangerous situations that they are about to face and that can cause human and material damages if not avoided. These situations are well identified and can be accidents/incidents on the road, traffic congestion in highways, approximation of narrow curves, tunnels or bridges, ice conditions on the road, a queue behind a curve, a vehicle that suddenly harshly brakes, the presence of vehicles in blind spots, etc. When facing all these situations, the driver can be assisted (Assisted Driving services) in order to take the appropriate behavior to avoid these hazardous situations and then improve road safety. For example, when there is a queue behind a curve or traffic congestion in highways, the driver can be informed to progressively reduce speed when approaching these dangerous situations or even to automatically control the vehicle speed reduction. Another example of assisted driving is when there is an accident on the road and the drivers are informed to take a specific behavior to improve the traffic flow on this spot. Other assistance examples that can be constantly provided to the drivers are the transmission of messages to maintain a safe speed, keep a safe distance, drive within the lane, safely pass intersections, avoid crashes with vulnerable road users, etc.

In this way, the information from these services can be provided in small messages (maximum of 1000 bytes) transmitted to all or specific vehicles in the vicinity of the RSU with a required maximum latency of 100 ms [41]. So, these types of services have low bandwidth requirements but are particularly demanding in terms of timeliness, since a late delivery of the messages compromises their usefulness.

7.2.2. Traffic Management

This type of V2I services convey information that may be useful to the drivers but have no direct impact on the safety. In this way, an information late delivery or even a delivery failure have no direct consequences in terms of human and/or material damages and therefore, these services don't exhibit the strong timing and reliability requirements like the V2I service types mentioned in previous subsection.

This type of services transports information related with the traffic management that can help the drivers to travel more comfortably on the roads improving the knowledge about situations beyond their environment that have impact on road traffic. As stated before, this information has no directed impact on safety but it can indirectly improve road security in some situations: if a road area suffers from a traffic congestion or bad weather conditions (rain, snow or frog), vehicles drivers that are approaching this area can be advised to take alternative paths and therefore there is less probability of happening accidents. So, some examples of road services that can be provided are road/weather condition warning, roadwork information, lane utilization information, speed limit information, area traffic congestion warning, current speed information, recommendation

about an alternative route e.g. related to driving direction indicating alternative paths where the traffic flow is better avoiding in this way problematic areas. Despite of not directly related with road safety, this type of information have some impact in terms of the drivers' road travelling quality and therefore a delivery failure will cause the drivers' to face inconvenient road situations.

So, this type of information should be given less priority than the one from Safety Warning/Assisted Driving which has a direct impact on road safety. The information related with these services can be also transported in small messages (maximum of 1000 bytes), thus, this type of service has low bandwidth requirements and low sensitivity to latency (less then 60 sec) [41], but exhibits some reliability requirements.

7.2.3. Commercial Applications

As the name implies, this type of V2I services was though to provide commercial applications on a user demand and therefore the information provided has no direct or indirect impact on road safety. In this way, it should be given a smaller priority than the two classes described above guaranteeing that it does not interfere in terms of timeliness, reliability or bandwidth with the road safety services.

This class of services is very broad, but is conceivable the coexistence of diverse road application classes or others. Some examples of services that can be provided in this class are individualised route guidance to help the drivers to take the correct path to reach a specific destiny, informing about the journey estimated time and using digital maps (similar to the service provided by GPS) or information about touristic points in the area where the drivers are travelling. It is also possible to assess the possibility of providing other services like multimedia (e.g. music, video), personal communications (e.g. VoIP) or generic Internet access (e.g. email, Web).

Thus, this class of traffic exhibits a mix of features; some services have high bandwidth requirements (e.g. video) while others have medium to low bandwidth requirements (travelling information or other); some services have no timeliness constraints (e.g. video feeds) while others are very sensitive to latency and jitter (e.g. VoIP).

7.3. V2I Applications Using WiMAX

The V2I service types described in the previous section should be provided using WiMAX and, therefore, it is necessary to assess this wireless technology in terms of the fulfilment of each specific service type requirements above identified.

The Safety Warning/Assisted Driving service types exhibit reliability and timeliness requirements and, in this way, this type of service should be provided in a WiMAX traffic class with real-time

properties since it is a traffic with an higher priority than any other one. The WiMAX service classes that give such type of guarantees are UGS and rtPS and therefore they should be used to provide V2I time-critical road safety services. The V2I Traffic Management services type is not demanding in terms of real-time issues and therefore it can be provided in non-real time WiMAX service classes to give priority to time critical V2I services. So, it should be provided using the nrtPS service class because, despite of not providing real-time properties, it provides reliability guarantees (this type of WiMAX QoS service gives bandwidth availability guarantees). The Commercial Applications services could be easily differentiated using the four service classes defined in the IEEE 802.16 – 2004. However, this type of services should not interfere with the time critical safety services, and therefore they will be provided in the nrtPS and BE WiMAX classes that don't give any real-time guarantees despite of some of them (like VoIP) having real-time requirements. It is possible to study, in the future, the coexistence of road safety critical services and commercial applications with real-time requirements using the same WiMAX class.

Using WiMAX, the information provided by the RSU can be transmitted to all vehicles (broadcast), to a specific vehicle (unicast) or to a group of vehicles (multicast) in the downlink direction. When a connection is established with an OBU, the RSU allocates a CID, which is the identifier of the information that the OBU should read. If a specific CID is allocated to all vehicles then the information transported in the SF associated will reach all vehicles. However, it is possible to allocate a CID to a group of vehicles or to a specific one to transmit individual information. In this way, it is possible for the RSU to transmit general safety information or to individualize and adapt the information to specific vehicles on the road (e.g., to prevent trucks to use certain roads).

Another aspect that can be considered is the fact that WiMAX allows the OBU's to communicate with the RSU to provide information about dangerous situations that the vehicles could have perceived. So, it is possible for the OBU's to ask for the creation of uplink connections to provide road security information to the infrastructure. These uplink connections should be also associated with a QoS service class and therefore it is also possible to prioritize the information provided by vehicles. For example, it is possible to have specific vehicles on the road which purpose is to perceive dangerous situation and inform the infrastructure (like the vision of COM2REACT project) and give them an higher priority than the information provided by general vehicles. In this way, it is also possible to assess WiMAX to perform V2V communication.

The Redline WiMAX BS used in this study only provides the rtPS and BE service classes and therefore the assessment will be only done using the rtPS class for time-critical services (Safety Warning/Assisted Driving) and BE for the others (Traffic Management and Commercial Applications). Also, this BS doesn't allow the creation of service flows by the SS and therefore it is not possible for the OBU's to ask for a specific connection creation. In this way, some tests were done to characterize the WiMAX system described above in terms of bandwidth, latency and jitter.

7.4. Tests Specification

In order to assess the suitability of WiMAX to provide the V2I services described above, it was

necessary to perform several tests to evaluate the overall system performance for this type of applications. As mentioned before, the tests were done using the developed WiMAX SS as an OBU and the Redline WiMAX BS as the RSU. However, some of these tests were repeated using the Redline WiMAX SS SU-O [42] to compare the results obtained using the developed SS with those obtained using a certified WiMAX SS equipment.

The tests performed were divided on two different categories: (1) Functional Tests and (2) Time Analysis Tests. The objectives of the Functional Tests are to evaluate the WiMAX system operation and throughput performance in optimal conditions, when both SS and BS are at fixed locations (both in laboratory and on the field) and to study the WiMAX RF link stability when the SS is moving at a constant speed relatively to the BS. The Time Analysis Tests were performed with the purpose of studying and characterizing the diverse WiMAX QoS service classes to conclude about their suitability to provide the V2I services described above, taking in account their specific delay and jitter requirements, using both Redline SS and WiRIA SS.

The WiMAX RF link characteristics used were the same for all the tests and consist on an operation frequency of 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.

7.4.1. Functional Tests

As stated before, these tests were performed with the objective of evaluating the correct behavior and data rate performance of the developed WiMAX SS, when both SS and BS are at fixed locations and then to characterize the link stability when the SS is moving at a constant speed of 30km/h relatively to the BS.

WiRIA SS Field Operational Tests

These tests had the purpose of evaluating the correct behavior of the WiRIA SS when used in a real deployment situation. The testing scenario is depicted in Figure 29. The BS was standing at a fixed location and the developed SS was placed fixed on different points at several distances from the BS with optical LOS. In all these points, the connectivity was verified and some parameters were measured to characterize the WiMAX link quality: (1) RSSI (provides a simple indication of how strong the signal is at the receiver front end), (2) CINR (a measurement of signal effectiveness), (3) Modulation and Codification used and (4) Network Entry process time. Next, in these same points, a throughput test was done by generating 1024 kbps and 10 Mbps UDP/IP traffic from PC1 to PC2 and vice-versa, measuring the data rate that reaches the receiver. The generation of the IP traffic is done using the open source software MGEN tool [43] which provides the ability to perform IP network performance tests and measurements using UDP/IP traffic.

The antenna used for the Redline BS was always the same having a 90º directionality (14 dBi gain). However, the antenna used for the SS was changed during these field tests. In all the tested points, an omnidirectional antenna developed at the Institute of Telecommunications was used but at

some points where the connectivity could not be established using this antenna, a Redline antenna with 15º directionality (18 dBi gain) was used instead.

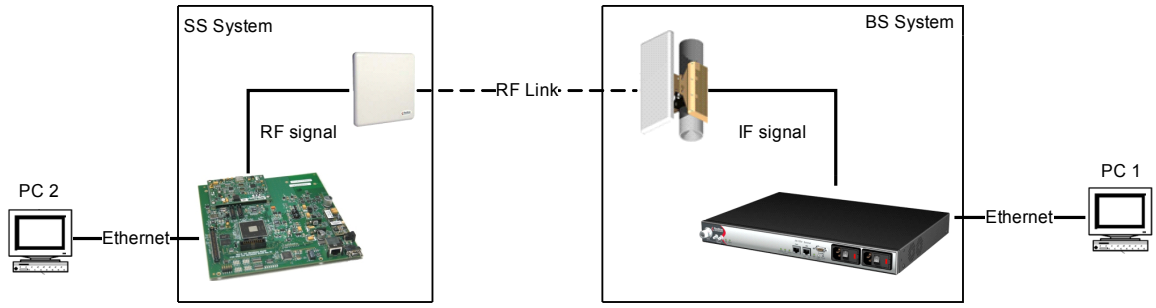

Figure 29: Field Tests Testing Scenario

Using this same scenario, some different tests were done when the SS is moving at a constant speed of 30 km/h relatively to the BS. In this case, only the omnidirectional antenna was used. These tests had the purpose of observing the maintenance of connectivity when the distance and propagation conditions between BS and SS are varying. The BS coverage area is limited due to the 90º antenna directionality and in this way, two different tests were performed: (1) the SS is already in the BS coverage area and performs the network entry process stopped and only after starts the movement; (2) the SS is turned on in a location out of the BS coverage area and then starts moving, performing the network entry process already in movement. To verify the maintenance of full connectivity during the movement, the ICMP ping was used performing echo requests from PC2 and waiting for the echo replies from PC1. In this way, it is possible to verify the connectivity in both downlink and uplink directions.

Throughput Characterization Tests

After evaluating the correct operation of the developed SS, an other test was done to verify the maximum allowed throughput by the WiMAX System. This test was first performed with the WiRIA SS and then repeated using the Redline SS SU-O to compare the results. The test scenario used was the same as represented in Figure 29 with the SS and BS at a distance of 10m.

To perform this throughput test, two WiMAX rtPS SF's were created between the WiRIA SS and BS, one for the downlink direction and another for the uplink direction. Next, using these service flows, a 256 kbps IP traffic was simultaneously transmitted (using MGEN) from PC1 to PC2 (downlink) and from PC2 to PC1 (uplink), using an IP packet length of 512 bytes, verifying the IP traffic data rate that reaches the receivers in both directions. This test was repeated for 512, 1024, 2048, 4096, 6144 and 8192 kbps (2 minutes each). Next, this test was repeated using BE SF's instead of rtPS ones. The tests described were repeated using the Redline SS.

7.4.2. Time Analysis Tests

These tests were performed to assess the suitability of the WiMAX system and associated QoS service classes, in terms of latency and jitter, to provide the already identified V2I Services. To perform this characterization, several simulated safety critical messages were sent through the

WiMAX System measuring their total latency. These messages were 1000 bytes long (maximum messages length for critical safety services) and were generated with a maximum period of 200 ms. All these tests were done using the developed SS and then repeated using the Redline SS.

As mentioned before, the Redline BS only provides the rtPS and BE class and therefore only those two can be evaluate. In this way, the BE delay measurement was first performed without any other traffic on the system and then this test was repeated for the rtPS class. Next, the BE delay was again measured but varying the rtPS traffic load on the system. For last, the rtPS delay was measured varying the BE traffic load on the system. In this way, it is possible to conclude about the real-time properties of the rtPS and BE class. All these tests are detailed next.

Only BE class on the system

This test purpose is to characterize the BE service class when there is no any other traffic on the system. To perform this, two BE SF's were created (one for DL and one for UL) that allow traffic from/to PC2 pass through the air. Using these two SF's, simulated safety critical messages were transmitted to measure the associated delay. Figure 30 shows the test scenario used and also depicts the time T1 which is the time since a message is sent from PC2 to PC1 plus the time of the associated response from PC1 to PC2 (round trip delay time).

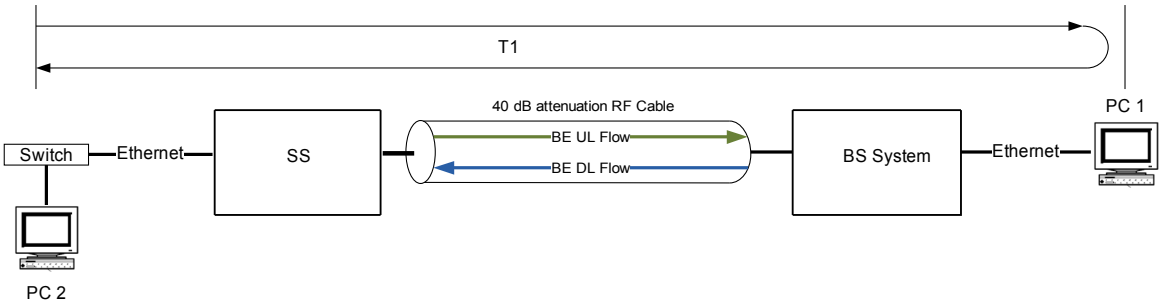

Figure 30: Test Scenario for measuring BE Delay alone

Only rtPS class on the system

This test is similar to the previous one but, in this case, two rtPS SF's (Figure 31) were created, instead of the BE ones, with the objective of characterizing the rtPS class with no other traffic on the system. The proceeding performed was the same, sending messages from PC2 and generating the respective responses from PC1 measuring the round trip time T1.

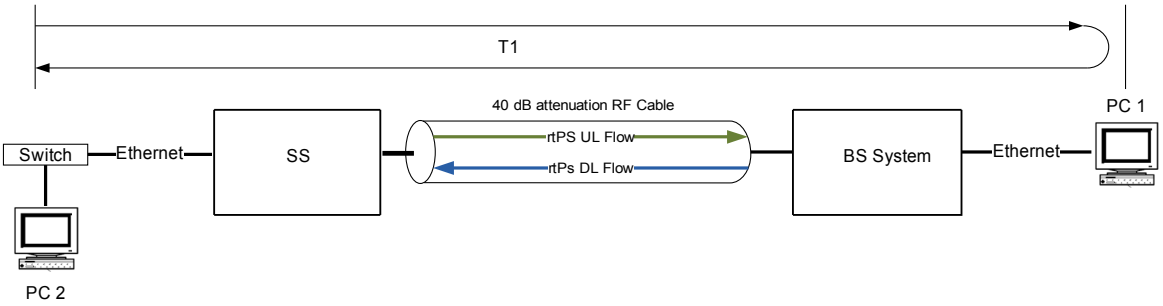

Figure 31: Test Scenario for measuring rtPS alone

BE Delay measurement with rtPS traffic on the system

In this test case, 4 SF's were created (Figure 32), two for the BE class (one UL and one DL) that allow traffic from/to PC2 pass through the air, and two for the rtPS class (one UL and one DL) that let the traffic to/from PC3 also pass through the air. Then, the simulated safety critical messages, that will be used to calculate T1, were transmitted in the BE SF's when, simultaneously, an IP traffic of 512 kbps was transmitted through the rtPS SF's (on both UL and DL) using MGEN. These T1 measurements were repeated for an rtPS IP traffic data rate of 1024, 2048, 4096 and 8192 kbps.

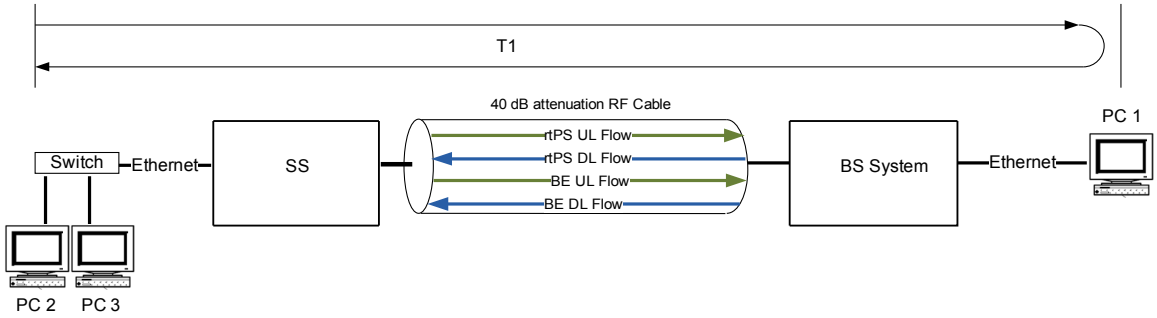

Figure 32: Test Scenario for measuring BE Delay with rtPS traffic on the system

rtPS Delay measurement with BE traffic on the system

This test was similar to the previous one but, instead of sending the messages through the BE SF's and varying the IP traffic on the rtPS SF's, the messages were sent through the rtPS SF's and the BE IP traffic was varied from 512 to 8192 kbps using MGEN and measuring T1 messages delay.

7.5. Tests Results

This section presents the results obtained from the tests described in the previous section. For each test performed, the results are shown and a critical analysis is done. The order by which the results are provided is the same as used in the specification.

7.5.1. Functional Tests

WiRIA SS Field Operational Tests

As mentioned in the tests specification above, this test had the purpose of verifying the correct operation of the WiRIA SS developed by performing several field measurements, with different distances among the SS and BS, and verifying the RF signal quality in both UL and DL. The results obtained are shown in Table 9.

Table 9: RF parameters measured in the Field Fixed Tests

Point	Distance to the BS (m)	CINR on the DL (dB)	RSSI on the DL (dBm)	CINR on the UL (dB)	RSSI on the UL (dBm)	SS antenna used	Network Entry Time (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

Observing Table 9 it is possible to see that the connectivity was always reached, using an omnidirectional antenna for points 1, 2, 3, 4 and 5 and a Redline 15º directional antenna for the other ones. The RF signal quality is good taking in account the RSSI and CINR values measured either in the UL and DL: all the CINR values measured are above 20 dB which indicates that the desired signal is strong compared to noise plus interference. The RSSI values measured show that the signal received in the 3.5 GHz band (this signal includes noise, interference and the desired signal) is also strong being always over -68 dBm. Another aspect that can be observed is the network entry process time which is always among 2 and 3 seconds. In this way, it is possible to conclude that the SS developed achieve a satisfactory connectivity with the BS with a good RF link quality signal, when both are fixed.

Table 10: Throughput measured in the Field Fixed Tests

Points	Distance to the BS (m)	Received Throughput for 1 Mbps generated Data Rate in DL (kbps)	Received Throughput for 10 Mbps generated Data Rate in DL (kbps)	Received Throughput for 1 Mbps generated Data Rate in UL (kbps)	Received Throughput for 10 Mbps generated Data Rate in UL (kbps)
1	31	849.3	-	991.65	-
2	71	991.26	5509.79	991.26	3855.42
3	78	855.6	-	991.23	-
4	98	991.23	-	990.68	-
5	140	854.68	-	971.8	-
6	200	863.41	5628.73	990.56	3682.12
7	240	991.44	-	991.85	-
8	330	852.15	5493.66	991.12	3602.94

Next, in all the points mentioned above, a throughput test was done by generating a 1024 kbps UDP/IP traffic data rate on the uplink and downlink simultaneously (using MGEN). This test was repeated using a UDP/IP traffic data rate of 10 Mbps in points 2, 6 and 8. The results are depicted

in Table 10.

Observing Table 10 it is possible to see the received data rate for each situation specified. When 1024 kbps data rate was transmitted, the received data rate is close to the generated one, either in the downlink and uplink directions. However, when 10 Mbps traffic data rate was generated, the received throughput was approximately 5.5 Mbps for the DL and 3.7 Mbps for the UL indicating the maximum allowed throughput for this WiMAX system, in these testing conditions.

After performing the field fixed tests, the movement tests specified in the previous section were done. When the SS started moving already registered, the connectivity with the BS was never lost, but, when the Network Entry process needed to be done already in movement, the connectivity was not established and therefore the creation of service flows was never done. So, it is possible to conclude that this WiMAX system, as implemented, is not adequate to a movement scenario. This problem can be related with the Doppler spread than can corrupt the orthogonality of the OFDM sub carriers making synchronization more difficult to achieve [18]. However, some studies shows that the Doppler spread can be limited by using directional antennas instead of the omnidirectional used in this test [44] and then further study can be done using the WiRIA SS in an movement environment. The directional antenna usage presents a disadvantage because the SS coverage area will be limited by the antenna breadth. Unfortunetly, this test could not be performed because the BS was not available being shared among several projects.

To conclude this part of the field tests results presentation, it is possible to say that the WiRIA SS shows a correct behavior when both BS and SS are at fixed locations. However, when the SS is moving relatively to the BS, the connectivity was not always satisfactory. When the network entry process needed to be done in movement, the connectivity was not reached. However, a study of the latency associated with the WiMAX service classes is required since it is possible to use the Mobile WiMAX which have the same defined QoS classes plus an extra one (ertPS) and already supports mobility. This mobility issue is related with the PHY layer used in Fixed WiMAX that does not provide the required features to support relative movement among the SS and BS, however, the PHY layer used by Mobile WiMAX should solve all this issues.

Throughput Characterization Tests

After evaluating the correct operation of the WiRIA SS, a throughput test was done. To compare the results, this test was repeated using the certified Redline SS. The results obtained using the WiRIA SS are depicted in Figure 33 and Figure 34 for the BE and rtPS class, respectively, for both DL and UL. The results using the Redline SS are shown in Figure 36 and Figure 35 .

Observing Figure 33 and Figure 34 it is possible to see that the WiRIA data rate received is similar using the rtPS and BE classes in both DL and UL. For the DL direction, the generated and received data rate is similar until reaching 5.5 Mbps of transmitted throughput approximately. After this, despite of increasing the generated data rate, the received one does not increase. The behavior for the UL direction is not very different from the DL direction but the maximum throughput is reached for approximately 3.8 Mbps.

The behavior for the Redline SS is similar to the one observed with the WiRIA SS. Observing Figure 35 and Figure 36 it is possible to see that, like in the WiRIA SS, the maximum allowed data rate is similar when using the BE and rtPS classes. In this SS, the DL direction allows a maximum throughput of approximately 5.5 Mbps while in the UL direction the maximum is 4.5 Mbps.

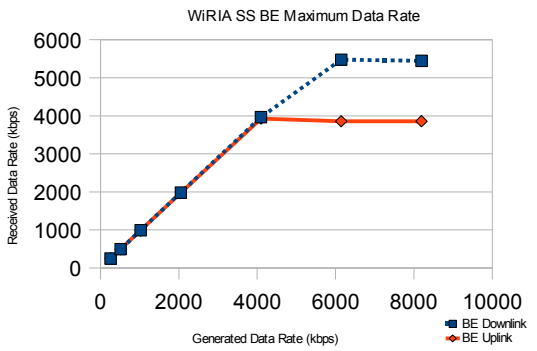

Figure 33: WiRIA SS Maximum Data Rate for the BE Class

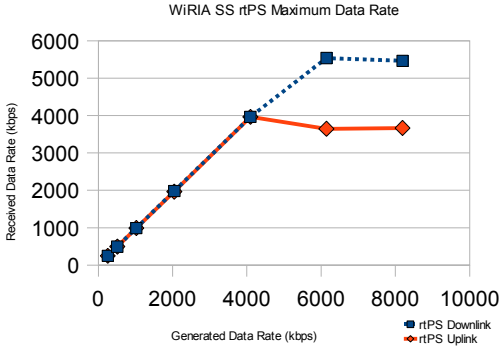

Figure 34: WiRIA SS Maximum Data Rate for the rtPS Class

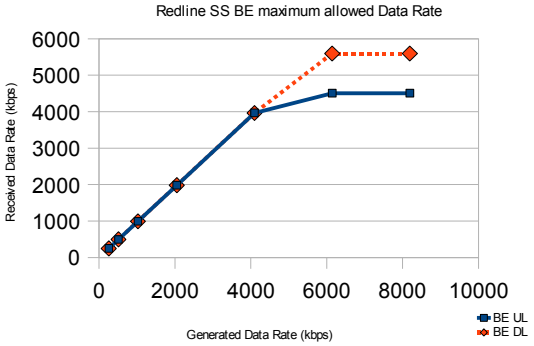

Figure 35: Redline SS Maximum Data Rate for the BE class

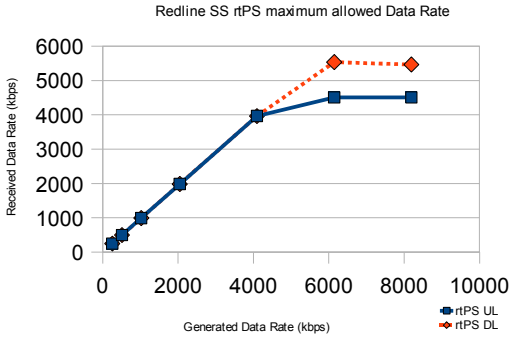

Figure 36: Redline SS Maximum Data Rate for the rtPS Class

So, it is possible to see that the maximum allowed throughput in DL and UL is similar using the Redline SS and WiRIA SS. It is even possible to see that, in the DL direction, the maximum allowed data rate is equal on both while in the UL direction the Redline SS allows a higher data rate (4.5 Mbps). The difference between the DL and UL throughput was expected because the ratio among the DL and UL sub-frame is 56% and 44% respectively. However, the higher throughput allowed by the Redline SS in the UL can be explained by an higher overhead of the WiRIA SS system when the packets are arriving with an high rate at the Ethernet interface, being then dropped.

7.5.2. Time Analysis Tests

After verifying the correct operation of the WiRIA SS and attesting its good throughput performance similar to a commercial certified Redline WiMAX SS, the time analysis tests specified were performed to assess the suitability of the WiMAX QoS classes to provide the identified V2I services.

Delay using the WiRIA SS

Table 11 shows the delay results obtained when the BE class of the WiRIA SS is used with different rtPS traffic loads on the system. Using the delay values measured, some other important parameters were calculated like the standard deviation and jitter (difference between the maximum delay and minimum delay).

Next, this same test was repeated for the rtPS class varying the BE traffic load. The results obtained are depicted in Table 12.

Table 11: BE Delay using the WiRIA SS

rtPS Data Rate on Both UL and DL (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 12: rtPS Delay using the WiRIA SS

BE Data Rate on Both UL and DL (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

It is important to refer that the delay measurements were also done using an 8192 kbps traffic load on both UL and DL but, in that case, all the delay values measured were so high that they were not considered (for both BE and rtPS).

To better understand the results shown in Table 11 and Table 12, some charts comparing the BE and rtPS classes for the different parameters calculated are presented next (Figure 37, Figure 38, Figure 40, Figure 39 and Figure 41). For all the parameters mentioned, it is possible to see that the rtPS class has a more constant behavior than the BE one which has a more rapidly increase of delay, standard deviation and jitter as the traffic load on the system increases.

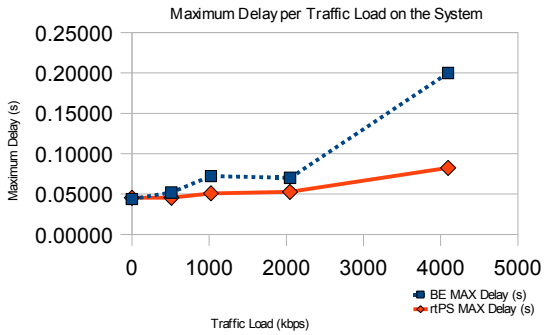

Figure 37: WiRIA BE and rtPS Maximum Delay

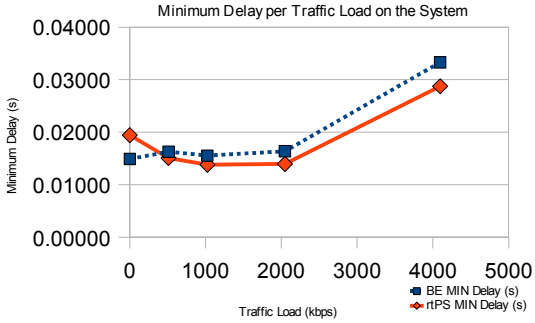

Figure 38: WiRIA BE and rtPS Minimum Delay

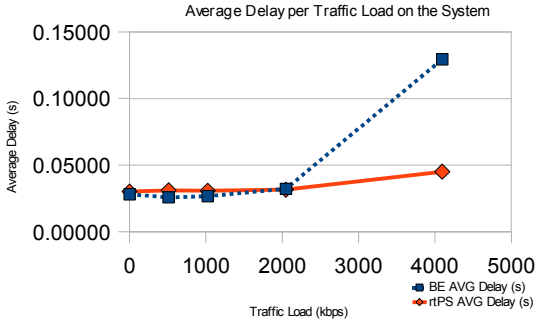

Figure 39: WiRIA BE and rtPS Average Delay

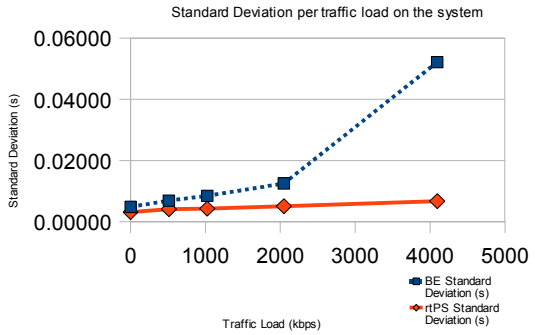

Figure 40: WiRIA BE and rtPS Standard Deviation

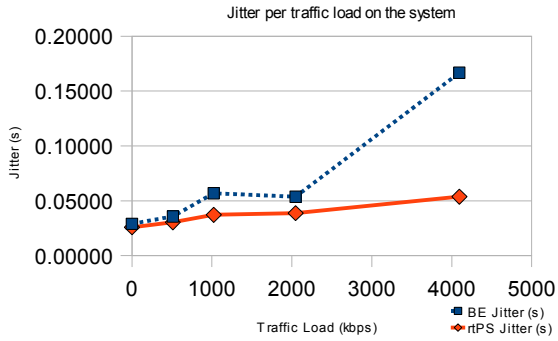

Figure 41: WiRIA BE and rtPS Jitter

Observing the charts previously mentioned, it is possible to see that, until reaching 2048 kbps of traffic load, the behavior of the BE and rtPS class is similar, presenting delay, standard deviation and jitter values that fulfil the safety services requirements. However, after passing this load level, the BE class has a rapid increase of the mentioned values while the rtPS class as only a minor increase, being almost constant. This indicates that the rtPS class, using the WiRIA SS, is suitable to provide Safety Warning/Assisted Driving services because the maximum delay measured is smaller than required (100 ms latency from infrastructure to car) , when the BE traffic load on both

UL and DL is not higher than 4096 kbps. On other hand, the BE class should not be used for safety services but it can provide Traffic Management or Commercial Applications services that don't have strong timeliness requirements. Another aspect that strengthens this though is the fact that the standard deviation and jitter for the rtPS class is small and almost constant when varying the BE traffic load, indicating that the rtPS class achieve a better predictability than the BE class, which as an intense increase of these values for rtPS traffic load above 2048 kbps.

A major drawback that was found using the WiRIA SS is the fact that, either for the BE and rtPS classes, the delay measured increases dramatically when there is a traffic load of 8192 kbps on both UL and DL. This indicates that this system is not suitable to provide V2I safety services when the system has such kind of load. So, some other delay measurements were done, for both rtPS and BE, generating traffic load of 8192 kbps first only on DL and then only in UL. Table 13 only shows the results for the rtPS class delay because the delay values measured for the BE class were again so high that they were not considered.

Observing Table 13, it is possible to see that the rtPS class has good real-time characteristics to provide V2I safety services when there is an intense load on the DL or on the UL. The maximum round-trip delay measured is much lower than the one required by V2I safety services and the standard deviation is small indicating a good predictability.

Table 13: rtPS Delay with 8192 kbps BE traffic load on DL and UL separately

	Maximum Delay (s)	Minimum Delay (s)	Average Delay (s)	Standard Deviation (s)	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

To conclude the WiRIA SS time analysis it is possible to say that, using the rtPS class, it is possible to fulfil the requirements of the V2I safety services (100 ms of delay in one way) and achieve a good predictability for certain type of usage scenarios: (1) when any BE traffic load is present only in DL or only in the UL and (2) when BE traffic load is smaller than 4096 kbps on both UL and DL. In these cases, the rtPS class exhibits delay values that are lower than 200 ms (the 100 ms delay specified for safety services corresponds only to the delay from infrastructure to vehicle) being then suitable to provide V2I safety services. The only situation that don't present adequate properties to provide safety services is when the traffic load on both UL and DL pass simultaneously 4096 kbps.

Delay using the Redline SS

In order to compare the performance of the WiRIA SS with the certified Redline SS (in terms of delay and jitter), the tests previously mentioned were repeated using this SS. The BE delay measurements using rtPS traffic load are presented in Table 14 while the rtPS ones using BE traffic load are depicted in Table 15.

In these tests, the delay measurements obtained when there is 8192 kbps of traffic load on both DL and UL were considered only for the rtPS class because their values were within acceptable delay

limits while the BE class ones were discarded because they have presented values that were extremely high taking in account the V2I services requirements specified. So, like in the WiRIA SS results presentation, some charts (Figure 42, Figure 43, Figure 44, Figure 45 and Figure 46) are presented to facilitate the comparison between the rtPS and BE classes when using the Redline SS.

Table 14: BE Delay using the Redline SS

rtPS Data Rate on Both UL and DL (kbps)	Maximum Delay (s)	Minimum Delay (s)	Average Delay (s)	Standard Deviation (s)	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
8192	0.20000*	0.20000*	0.20000*	0.02000*	0.20000*

* The values measured for 8192 kbps were so high that they were not considered. The values that are present on the table have the only purpose of showing the intense degradations of the BE class with 8192 kbps of rtPS load

Table 15: rtPS Delay using the Redline SS

BE Data Rate on Both UL and DL (kbps)	Maximum Delay (s)	Minimum Delay (s)	Average Delay (s)	Standard Deviation (s)	Jitter (s)
0	0.05197	0.01996	0.03428	0.00642	0.03201
512	0.4794	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

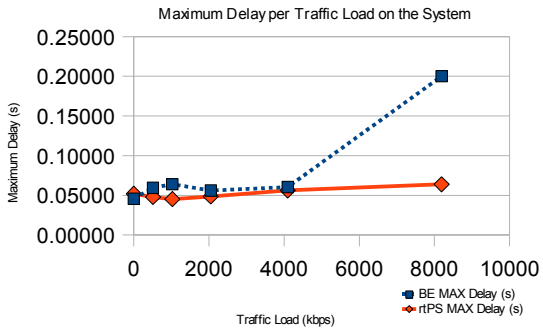

Figure 43: Redline BE and rtPS Maximum Delay

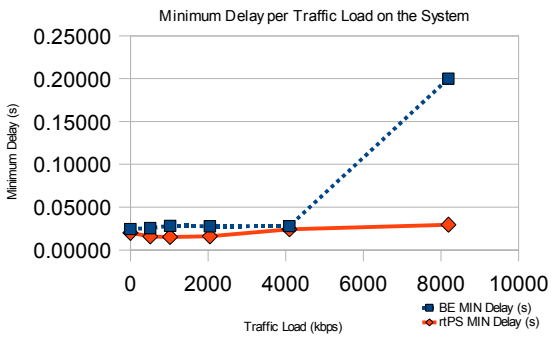

Figure 42: Redline BE and rtPS Minimum Delay

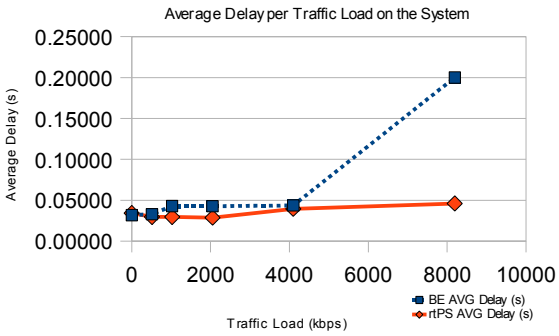

Figure 44: Redline BE and rtPS Average Delay

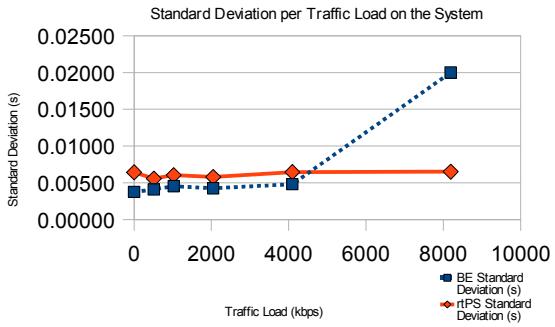

Figure 45: Redline BE and rtPS Standard Deviation

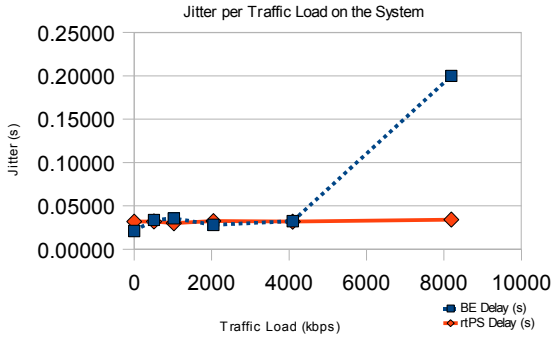

Figure 46: Redline BE and rtPS Jitter

Despite of not being considered, the BE delay values obtained when there is 8192 kbps rtPS traffic load were represented in the charts previously mentioned to give the perception of the degradation of the BE class relatively to the rtPS one. So, it is possible to see that the general behavior of this SS is similar to the one observed with the WiRIA SS, however, some small differences can be noticed. First, it is possible to see that the behavior of the rtPS and BE class is similar until reaching a traffic load of 4096 kbps on both DL and UL. For higher traffic loads, an intense degradation of the BE class is visible while the rtPS maintains its good real-time properties for any kind of traffic load on the system.

Then, it is possible to conclude that, using the Redline SS, the rtPS class has good characteristics to provide safety critical services because, despite of increasing the BE traffic load on the system, the rtPS delay, standard deviation and jitter do not increase being almost constant and fulfilling the safety services delay requirements. It is also important to say that, unlike the WiRIA SS, if the traffic load on both DL and UL is superior to the one allowed by the WiMAX system, the rtPS class maintains its real-time properties, being then suitable to provide safety services independently of the BE load on the system.

Redline SS vs WiRIA SS

After describing the real-time properties of the WiRIA and Redline SS's, it is possible to compare their performance. So, as mentioned before, it is possible to see that the rtPS class, on both SS's, has a better real-time behavior than the BE class which has an higher delay degradation as the traffic

load on the system increases. This BE effort delay degradation is visible when the rtPS traffic load is above 2048 kbps on the WiRIA SS and 4096 kbps on the Redline's. Another aspect that can be noticed is that the rtPS class, using Redline SS, maintains its good real-time properties even when the BE traffic load on the system is intense on both UL and DL. This behavior is not similar on the WiRIA SS which exhibits rtPS high delays when the BE traffic on both DL and UL is 8192 kbps. However, when this traffic load is only in DL or only in UL, the rtPS has delay values that make it possible to be used for safety critical services.

So, the tests performed lead to the conclusion that the Safety Warning/Assisted Driving services can be provided using the rtPS QoS class with both SS's with some constrains when the WiRIA SS is used. Using the certified Redline SS, the real-time properties are maintained independently of the BE traffic load on the system while using the WiRIA SS, these services should not be provided when the traffic load on the system is higher than 4096 kbps on both DL and UL. The Traffic Management and Commercial Application can be provided using the BE class because they do not exhibit strong requirements.

7.6. Conclusions

This chapter has presented the different services to be provided using an infrastructure to vehicle communication. This V2I services were divided in three different categories: Safety Warning/Assisted Driving, Traffic Management and Commercial Applications, each one with its specific requirements. The Safety Warning/Assisted Driving presents very strict reliability and timing requirements while the Traffic Management services are not demanding in terms of timeliness but presents reliability requirements. For last, the Commercial Applications have different real-time requirements but since it is not a safety critical service, it should be given less priority than the two previous ones.

After mentioning the requirements of the different V2I services, the tests that were done to assess a WiMAX system for this type of communication were explained. First, some functional tests were done to the developed SS to evaluate its correct operation, either with the SS fixed as well as moving. These tests allowed to conclude that the WiRIA SS has a good operation when fixed but presents some problems when moving, in particular when it needed to perform the network entry process already in movement. After these tests, others were done to assess the WiMAX QoS classes to provide the safety critical services using both the WiRIA SS and Redline SS. These tests have shown that the WiMAX rtPS service class, using the WiRIA SS have good properties to provide the safety services mentioned when there isn't BE throughput higher than 4096 kbps on both DL and UL. The rtPS class, using the Redline SS, can be used without any BE traffic limitation to provide safety services.

Chapter 8

Conclusions and Future Work

8.1. Conclusions

The dramatic impact that road accidents have on the society is fostering the research of mechanisms for increasing road safety. Most of the approaches that are being developed depend on the ability of the vehicles to communicate with each other and/or with fixed roadside equipments. So, many initiatives are being carried out to develop the mentioned mechanisms and specifically in Europe, many projects are being funded by the European Commission to develop Intelligent Vehicles Systems with the purpose of reducing road injuries and fatalities.

The heterogeneous set of requirements imposed by the diverse V2I applications is extremely demanding with respect to the underlying wireless infrastructure. This dissertation presented a work on the development of a WiMAX SS, in the scope of the WiRIA project, and assessed the

suitability of the WiMAX wireless technology to provide vehicular communication services. This SS was based on a FUJITSU development kit that already implemented the PHY and MAC layers of WiMAX, however, several changes were made to improve its behavior creating a real WiMAX solution.

So, to assess the WiMAX technology to be used in a vehicular communication scenario, the V2I services to be provided were presented and their specific requirements were detailed. These services were divided in three categories: (1) Safety Warning/Assisted Driving that present strict timing and reliability requirements, (2) Traffic Management that are not demanding in terms of timeliness but present some reliability requirements and (3) Commercial Applications that exhibit a mixture of requirements but that should not interfere with safety services.

The WiMAX vehicular communication assessment was done using the developed WiRIA SS and a WiMAX Forum certified Redline SS. So, the correct operation of the WiRIA SS was first verified by performing some field tests, both fixed and mobile. These tests have shown that the WiRIA SS has a correct operation when fixed at a specific location but presented some problems when the Network Entry process needed to be done moving at a constant speed of 30 km/h relatively to a fixed BS. In this way, it is possible to conclude that the WiRIA SS, as implemented, does not provide a correct behavior in a moving environment, fact that was already expected but that the Mobile WiMAX version should solve. The mentioned problems are related with the PHY layer and can be caused by the rapid variation of the propagation conditions and by the Doppler effect that results on a frequency deviation that can lead to a SS non synchronization, process which is done on the Network Entry process. After performing the movement test, a throughput one was done to both SS's and it was verified that, for the same WiMAX link properties, the WiRIA SS and Redline SS have a similar DL maximum allowed throughput (~5.5 Mbps) but the WiRIA SS presents a smaller UL maximum throughput (3.8 Mbps) than the Redline SS (4.5 Mbps). This difference can be explained by a non optimization of the WiRIA SS software when the data rate that arrives to the Ethernet interface is intense.

Some tests were done to verify the WiMAX QoS classes' adequation to provide the V2I services identified. This assessment was done using both Redline and WiRIA SS's to compare the results. In this way, the tests performed with the WiRIA SS permits concluding that the WiMAX rtPS service class can be used to provide V2I safety critical services for BE traffic loads not higher than 4096 kbps on both DL and UL. However, using the certified Redline SS, the results have shown that the rtPS class always provides an adequate behavior, independently of the BE load on the system. In this way, it is possible to say that the rtPS class provides sufficient guarantees to provide V2I safety service while the non safety critical services can be provided by the BE class.

8.2. Future Work

The work performed on this dissertation indicates that WiMAX has good potential to be used in vehicular scenarios to deliver safety critical information and other, providing adequate traffic differentiation. However, some further investigation need to be done to understand which are the

options that can be pursued on this context.

One possible choice that can be made is to assess Fixed WiMAX equipment to be used in specific movement scenarios. This dissertation has concluded that the WiMAX QoS service classes present good characteristics to provide V2I services and, in this way, it is possible to evaluate Fixed WiMAX equipment to be used in specific vehicular scenarios. As mentioned before, the WiRIA SS, as implemented, did not work well when the network entry process should be done in movement using an omnidirectional antenna. Further investigation can be done using directional antennas that reduce the Doppler spread and study and overcome the limitations of the PHY layer in this type of scenarios. Other subjects that need to be studied is the Network Entry process and the service flows creations times, when there is a relative movement among the BS and SS. The usage of Fixed WiMAX equipment for specific movement scenarios has the advantages of being cheaper and a less complex technology than Mobile WiMAX, being then suitable to provide communication between infrastructure and vehicles in specific points like narrow curves, tunnels, bridges, etc.

Another path that can be taken is to use Mobile WiMAX equipments. The IEEE 802.16e defines five QoS service classes, the same four as defined in the IEEE 802.16d standard plus and extra one: ertPS. The Mobile WiMAX version uses the OFDMA PHY layer and supports several key features necessary for delivering mobile broadband services at vehicular speeds greater than 120 km/h [45], being then suitable for vehicular communication scenarios. The four QoS service classes are defined exactly the same way on both standards and therefore the time analysis (rtPS and BE classes) results from this dissertation are valid for the Mobile WiMAX. However some further study should be done by evaluating the five QoS scheduling classes of Mobile WiMAX and understanding the times associated with the Network Entry, service flow creations and handover processes. The usage of Mobile WiMAX can be though for creating a continuous link with the road, being then possible to provide continuously information to the vehicles. In 2008, the first mobile equipments are appearing in the market and there is already some certified products by the WiMAX Forum.

Another aspect that should be studied in the future is a WiMAX communication scenarios using multiple SS's in a PMP environment, situation that will appear commonly on the road. It is necessary to understand the implications of the usage of several SS's in terms of the QoS service classes and processes times.

References

[1] Ministério da administração Interna, "Sinistralidade rodoviária 2006", Elementos estatísticos 2007, http://www.mai.gov.pt/ visited in October 2007.

[2] eSafety Forum, "Europe's Information Society", http://ec.europa.eu/ information_society /activities/ esafety/index_en.htm visited in November 2007.

[3] F. Karl, "Vehicular Communications and VANETS", ULM University 2006 presentation.

[4] IEEE 802.16 Working Group, "The IEEE 802.16 Working Group on Broadband Wireless Access Standards", http://www.ieee802.org/16/ visited in December 2007.

[5] WiMAX Forum (2008), http://www.wimaxforum.org, visited in December 2007.

[6] eSafety Forum, "Europe's Information Society", http://ec.europa.eu /information_society/activities/ esafety/index_en.htm visited in November 2007.

[7] i2010 Intelligent Car Initiative, "Welcome to Intelligent Car Initiative" http://ec.europa.eu/ information_society/activities/intelligentcar visited in December 2007.

[8] CORDIS Europe, "FP6 - Sixth Framework Program", http://cordis.europa.eu/fp6/fp6_glance.htm visited in January 2008.

[9] COMeSafety, "Communications for eSafety", http://www.comesafety.org visited in January 2008.

[10] COOPERS, "Co-operative Systems for Intelligent Road Safety", http://www.coopers-ip.eu visited in January 2008.

[11] SAFESPOT, "Cooperative vehicles and road infrastructure for road safety", http://www.safespot-eu.org visited in January 2008.

[12] CVIS, "Cooperative vehicle-infrastructure Systems", http://www.cvisproject.org visited in January 2008.

[13] C2R, "COM2REACT", http://www.com2react-project.org visited in January 2008.

[14] PREVENT, http://www.prevent-ip.org, visited in January 2008.

[15] SEVECOM, "Security on the Road", http://www.sevecom.org visited in January 2008.

[16] VII Project, http://www.its.dot.gov/vii/ visited in January 2008.

[17] IEEE 802.16 Working Group, "The IEEE 802.16 Working Group on Broadband Wireless Access Standards", http://www.ieee802.org/16/ visited in December 2007.

[18] J.G. Andrews et al, "Fundamentals of WiMAX", Prentice Hall 2007.

[19] IEEE 802.16 Working Group, "Standard 802.16-2004. Part16: Air interface for fixed broadband wireless access systems".

[20] WiMAX Forum White Paper, "The WiMAX Forum Certified Program for Fixed WiMAX".

[21] IEEE 802.16 Working Group, "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", IEEE.

[22] WiMAX Forum White Paper, "Mobile WiMAX—Part I: A technical overview and performance evaluation", WiMAX Forúm.

[23] WiMAX Forum (2008), http://www.wimaxforum.org visited in December 2007.

[24] Eklund, C., Marks, R., Ponnuswamy, S., Stanwood, K. L., and Waes, N., "WirelessMAN, Inside the IEEE 802.16TM Standard for Wireless Metropolitan Networks", Standards Information Network IEEE Press 2006.

[25] Perdo Neves, "Qualidade de Serviço em Redes de Acesso IEEE 802.16", Universidade de Aveiro 2006.

[26] Louftani Nuaymi, "WiMAX technology for broadband wireless access", ENST Bretagne,France, 2007.

[27] IT, "Instituto de Telecomunicações", http://www.it.pt visited in November 2007.

[28] ASPEX WiMAX Development Kit, http://www.aspex-semi.com/pages/products visited in November 2007.

[29] Fujitsu Microelectronics America (fma), http://www.fujitsu.com/us /services/edevices/ microelectronics visited in November 2007.

[30] Fixed WiMAX - 802.16-2004 SoC (MB87M3550), http://www.fujitsu.com /us/services/edevices /microelectronics/broadbandwireless/products/visited in November 2007.

[31] Intel, http://www.intel.com visited in November 2007.

[32] Intel WiMAX Products, http://www.intel.com/technology/wimax/products.htm visited in November 2007.

[33] Sequans Communications, http://www.sequans.com/ visited in November 2007.

[34] Sequans Communications – Fixed WiMAX(2008), http://www.sequans.com /products /fixed_wimax.php, visited in November 2007.

[35] TeleCIS Wireless (2008), http://www.telecis.com/ visited in November 2007

[36] Wavesat (2008), http://www.wavesat.com/home.php visited in November 2007

[37] Redline Communications, http://www.redlinecommunications.com visited in November 2007

[38] Intel IXP425 (2008), http://www.intel.com/design/network/products/ npfamily/ixp425.htm visited in November 2007.

[39] Fujitsu Microelectronics, "MB87M3550 Fujitsu WiMAX 802.16-2004 SoC Programming Guide".

[40] GoAhead, "WebServer Overview", http://www.goahead.com/products/webserver/ default.aspx visited in February 2008

[41] Coopers–Co-operative Systems for Intelligent Road Safety, "GPRS and V2I communication", Dr.J.H. Linssen, 20 June 2007, Aalborg ITS.

[42] Redline Communications, "RedMAX SU-O", http://www.redlinecommunications.com/products/RedMAX_SUO.html visited in visited in February 2008

[43] Networks and Communication System Branch, Naval Research Lab, Washington, "Multi – Generator (MGEN)", http://cs.itd.nrl.navy.mil/work/mgen/ visited in February 2008

[44] George Zaggoulos, Andrew Nix, Angela Doufexy, "WiMAX System Performance in highly mobile scenarios with directional antennas", Centre for Communications Research, University of Bristol, United Kingdom.

[45] Doug Gray, "Mobile WiMAX, Performance and Comparative Summary", WiMAX Forum,, September 2006,