# WAYMAX@VANTAGE SYSTEM: THE SIEMENS PLATFORM FOR DELIVERING PACKET-BASED DATA/VOICE SERVICES BASED ON THE WIMAX/IEEE802.16 STANDARD

**Alessandro Nevola, Luigi Lovino**

*Siemens Networks S.p.A. – Carrier Research and Development Microwave – Cassina de' Pecchi, Milano (Italy)*

Abstract: During the last years the quest for new wireless technologies has driven the efforts of telecommunications companies and standardization groups. WiMax (Worldwide Interoperability for Microwave Access) has arisen as the most promising of the new technologies for providing access to fixed/nomadic subscriber stations. It was standardized by the IEEE 802.16 group in 2004 and it is well suited to the last mile broadband wireless access.
In the present paper the WiMax Siemens solution, a highly scalable multi-sector platform, is described in some details. In particular we focus on the services that can be provided and on the functional description of the Base Station.


Keywords: WiMax, fixed broadband wireless networks, metropolitan area network, microwave, OFDM

## 1. INTRODUCTION

The Wimax/IEEE802.16 standard [1] provides a potentially cost effective solution for connecting residential and small/medium business Users to the local Operator point of presence, delivering broadband wireless access in the last mile. As demonstrated by the first network deployments, the technology is today mature enough to satisfy the increasing demand for internet based services, still keeping the cost competitive with the existing DSL-based networks. The Standard offers the possibility to provide service to fixed/nomadic and, in the near future, to mobile Users, overcoming the limitations of legacy access technologies. Besides being a great possibility for new entrant Operators to compete with existing incumbents, this WiMAX solution is also a possibility for the incumbents to improve network coverage in the last mile, providing broadband services to those Users who cannot be reached by means of the traditional copper-based connections. The general interest in this technology is demonstrated by the standardization activity of the last years by the IEEE and ETSI standardization groups.

Siemens WiMAX platform named "WayMAX@vantage" is the solution offered by Siemens to Operators that want to face this challenge. The Siemens WayMAX@vantage System has been certified by the WiMAX Forum on the 17 March 2006, and is intended to provide full interoperability with other vendors based on the IEEE 802.16-2004 standard.

The present article provides a description of the WayMAX@vantage System, its applications and its architecture.

## 2. SIEMENS WAYMAX@VANTAGE SYSTEM

Siemens provides an in house made solution for both Base Station (BS) and Customer Premises Equipment (CPE). The Base Station architecture supports FDD and TDD modes of operation. A support to H-FDD CPE is also provided by the BS. The equipment has a split Indoor unit / Outdoor unit architecture, being the Indoor unit completely frequency independent. The Outdoor units cover the 3.4÷3.8 GHz frequency bands for the FDD mode, and the 2.3÷2.5 GHz frequency band for the TDD mode.

The Siemens Customer Premises Equipment is a low cost compact desktop equipment with low directivity antenna; the duplex mode is H-FDD.

### *2.1. Services*

The Base Station provides service to several CPE located in a squared or rounded region around the Base Station, in a typical Point to Multipoint access system. The Siemens low cost Customer Premises Equipment provides network connection to a single residential or business User or to a group of co-located residential Users in a multi-dwelling environment. The propagation conditions between the Base Station and the CPE may be non-line-of-sight [2].

The connections dedicated to each User may be configured to provide the suitable quality of service for several types of packet-based services. At present voice services, the VoIP, and data services, e.g. Internet browsing, are possible for residential Users. Also interconnection of small/medium size business Users may be supported by means of a sort of Virtual Private Network extended to the access area.

To support this multiplicity of services/applications, different service classes are provided by the System, as required by the Standard: the Best Effort, the non real time Polling Service, and the real time Polling Service classes are available and may be bounded to every User interface to satisfy its needs in terms of capacity, time latency and traffic priority.

### 2.2. *The "nomadic" user*

The present time WayMAX@vantage system is based on the IEEE 802.16-2004 recommendation, the fixed part of the standard. Nevertheless two different types of Users may be served: the "provisioned" and the "nomadic" Users. In the "provisioned" configuration the Base Station accepts only Users who have been previously configured in the Base Station configuration database. Provisioned Users have a predefined quality of service with multiple connections, to support different services each with the right quality. In the "nomadic" configuration a CPE is accepted by the Base Station even if "unknown"; in such a case a reduced Quality of Service is provided to this User. This "nomadic" configuration allows a User to move from a radio Sector to another radio Sector inside the same Base Station or from a Base Station to another, without being previously registered by the Operator. A "mixed" configuration is allowed by the Base Station where each User is provisioned on a predefined Base Station with a full QoS, but he can move and gain access to the network on every other Base Station as a "nomadic" User, with a reduced best effort QoS. In either case, Security is guaranteed when the User enters the network by means of the PKMv1 Security scheme compatible with the 802.16 standard.

### 2.3. *Nomadicity and Qos*

The support to nomadic users as described in paragraph 2.2 allows the Network Operator to manage the nomadicity in the easiest possible way. The cost of that simplicity is the lack of Qos for the nomadic user. However, the BS provides a feature to overcome this limitation: It is possible to activate a RADIUS client ([3]) on the BS, which acts now as a NAS (Network Access Server) for the CPEs. In this scenario the configuration of the CPEs (e.g. traffic connections with an agreed Qos) is centralized in the database associated with the RADIUS server. The nomadic user can have his own Qos when he moves from BS to BS, provided that the RADIUS server is available to every BS of the network. Moreover the RADIUS server offers an Accounting service as well.

### 2.4. *Network Interfaces*

The System provides a packet based interface, both User side and Network side. By now an Ethernet Interface is provided on both sides. The high data rate 1000BaseT and 1000BaseFx interfaces are possible on Network side, while a 10/100BaseT interface is provided on User side.

### 2.5. *Management Interfaces*

The supervising of network functionality is recognized as one of the most critical issue in the modern network environment, where equipment from different vendors coexists side by side. In view of that, SNMP, a "de facto" standard, has been implemented for the management plane.
In order to provide maximum flexibility to the Network Operator, three different management interfaces are foreseen:

- In-Band Interface, Ethernet 10/100/1000 BaseT, which coincides with the traffic interface
- Out-of-Band Interface, Ethernet 10/100 BaseT, to be connected to a TMN
- Local Management Interface, Ethernet 10 BaseT, available for in field O&M activities

Managed CPEs can be reached via In-Band and Out-of-Band Interfaces. With the aim of simplifying the assignment of the CPEs IP addresses, a DHCP Server/Relay Agent is embedded in the BS.

### 2.6. *Protocol layers descriptions*

*Reference Model.* The protocol reference model is based on IEEE 802.16-2004 standard, i.e. a layered model composed of:

- Service-Specific Convergence Sublayer (CS)
- MAC Common Part Sublayer (MAC CPS)
- Security Sublayer
- Physical Layer (PHY)

CS and PHY layers offer different choices to the designer: Due to the growing importance of the packets networks, the Packet CS has been implemented; NLOS radio functioning is achieved by adopting OFDM PHY layer.

As the Radio Interface is intrinsically more vulnerable than wired networks, e.g. to eavesdroppers attack, particular care has been taken in the design of the Security sublayer.
The functions involved in the Security sublayer include [4]:

- CPEs authorization by means of X.509 certificates
- Authorization Key exchange (RSA encrypted)
- HMAC Digest MAC messages validation
- Traffic Encryption Key exchange (RSA, Triple-DES or AES encrypted)
- Data traffic Encryption (DES in CBC mode or AES in CCM mode)

*Radio Physical Layer.* The communication between the Base Station and the CPEs is based on either a FDD/TDMA or a TDD/TDMA scheme: in both cases, downlink and uplink data streams will be a sequence of Bursts, each one allocated in a predetermined part of the downlink or uplink sub-frame and spanning an integral number of OFDM Symbols.

In the upstream direction the association between the OFDM Symbols and the related CPEs will be determined by the Base Station by means of a "Centralized Scheduling Algorithm", avoiding collisions between CPEs requiring access at the same time.

Efficient bandwidth usage is assured by packing and fragmentation of Ethernet frames (in the MAC layer) and concatenation in the same physical Burst of MAC PDU belonging to different connections using different Classes of Traffic.

In Figure 1 an example of Packing with Fragmentation, Fragmentation of long SDU and Concatenation is shown.

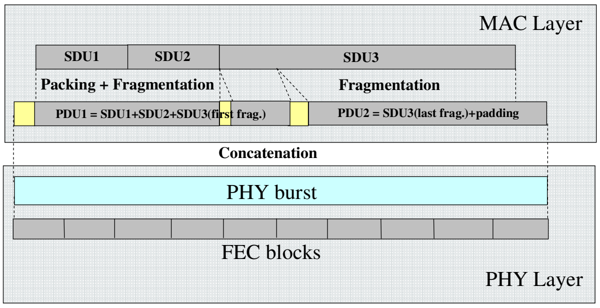

Fig. 1. Packing, Fragmentation and Concatenation

As already told, the modulation is based on OFDM technique with Cyclic Prefix: this transmission system, together with channel encoding comprising interleaving in the frequency domain and concatenated Reed-Solomon and Convolutional FEC, allows NLOS (Non Line Of Sight) operations [5]. The system robustness to NLOS conditions has been tested in lab with SUI-3 and SUI-4 channel models and then confirmed in a real life environment.

In Table 1 the concatenated FEC for all the Physical Modes is shown, along with the spectral efficiency in b/s/Hz.

Table 1 Physical modes code rate and spectral efficiency

| PHY Mode | Mod. | RS code rate | CC rate | Overall code rate | Efficiency [b/s/Hz] |
|---|---|---|---|---|---|
| 0 | BPSK | (12,12,0) | 1/2 | 1/2 | 0.4 |
| 1 | QPSK | (32,24,4) | 2/3 | 1/2 | 0.8 |
| 2 | QPSK | (40,36,2) | 5/6 | 3/4 | 1.2 |
| 3 | 16QAM | (64,48,8) | 2/3 | 1/2 | 1.6 |
| 4 | 16QAM | (80,72,4) | 5/6 | 3/4 | 2.4 |
| 5 | 64QAM | (108,96,6) | 3/4 | 2/3 | 3.2 |
| 6 | 64QAM | (120,108,6) | 5/6 | 3/4 | 3.6 |

*Physical Layer Management.* Physical layer management is performed by means of MAC CPS messages transported on Basic, Primary and Broadcast connections (these connections are created automatically by the BS). This scheme allows centralized control of the RF electronics and basic configuration of the CPEs. In this way it is possible to share the Radio Interface among dozens of CPEs without disrupting the services one another.

Moreover, an integrated ATPC/Adaptive Modulation mechanism, based on accurate RSL and CINR measurements, maximizes both radio interface capacity and coverage.

For these purposes, the physical layer management is characterized by the following functions:

CPE Admission in the Radio Sector (Network Entry):

- Equalisation of TX Power and Propagation Delay (Initial Ranging)
- Basic capabilities mutual agreement, Authorization and Registration
- Traffic connections set-up and Parameters Configuration

Refresh of CPE parameters and configuration:

- Periodic Ranging
- Adaptive Modulation and ATPC control
- Change of connection parameters, e.g. MSTR for BE connections

Encryption Procedure Control:

- Re-Authorization
- Keying material renewal

### *2.7. System Architecture*

The system functional architecture is based on a distributed Layer 2 Bridge, with IEEE 802.16-2004 compliant radio interface towards CPEs, which can be configured in bridged or in routed mode. As any standard IEEE 802.1d bridge, forwarding, static entry creation and learning functions are implemented.

The main functional blocks of the BS are:

- CSU (Control Switch Unit)
- SMU (Switch Modem Unit)
- ODU (Out Door Unit)
- CU (Connector Unit) Power Supply and synchronization connectors

The CSU is the control unit of the entire BS. It hosts the Network Interface which is usually connected to an IP router in the ISP access network. Its main duties are:

- Traffic switching towards Radio Sectors (based on destination MAC address)
- Alarms gathering
- Redundancy control

- SNMP agent and permanent storage of configuration data (MIB)

In Figure 2 the functional architecture of the Base Station is shown.

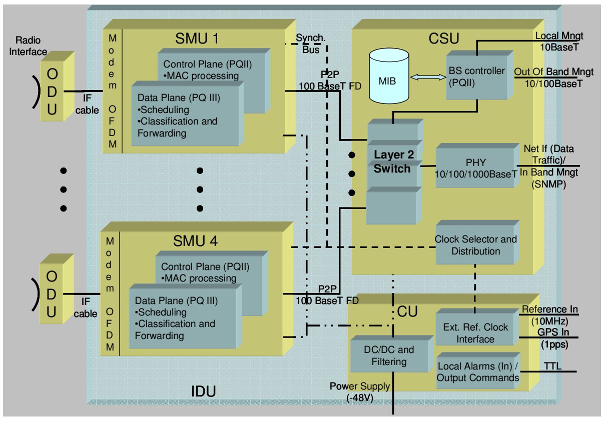

Fig. 2. BS system functional architecture and interfaces

The SMU is responsible for the PHY and MAC Layer processing inside a single Radio Sector. Besides, it realizes the "aerial" part of the Bridge: every incoming packet is forwarded to the relevant CPE according to the filtering database information. In order to guarantee a defined Quality of Service, a VLAN Priority or IP TOS based classifier maps the downlink traffic to the appropriate Service Flow.

The SMU is connected by means of a single coaxial IF cable to an RF ODU containing the microwave parts.

*IDU Physical Structure.* The physical structure of the Indoor Unit is composed of one standard (ETSI/19") Subrack.

The IDU supports a wide range of outfits: from the simplest (one CU, one CSU and one SMU) to the most complete, composed by two CU, two CSU and five SMU.

The main building blocks of CSU card are:

- Freescale PowerQUICC™ II Micro Processor (System Controller)
- Marvell™ Ethernet Switch (data switching)
- Compact Flash memory card
- Ethernet Interface Controller (10/100/1000 BaseT or FX, 10/100 BaseT, and 10 BaseT)

The SMU mainly provides the following functionalities: the DLC (Data Link Controller) and the OFDM Modem.

The DLC, which implements in Software the MAC layer, is composed by:

- Freescale PowerQUICC™ III Micro Processor for Data Plane (data switching)
- Freescale PowerQUICC™ II Micro Processor for Control Plane (MAC management)
- TCAM (Ternary Content Addressable Memory) for efficient search engine implementation
- Ethernet Interface Controller (100BaseT towards CSU and Modem)

The OFDM Modem is realized in FPGA and DSP technology.

*Outdoor Unit.* The Outdoor Unit (ODU) is composed of the whole microwave parts (including IF / RF conversion and synthesizer).

The connection towards the IDU is done by means of a single coaxial cable, carrying frequency division multiplexed IF main signals (uplink and downlink) and telemetry channel for ODU control. The power supply is provided by the IDU via coaxial cable as well. Main technical choices are:

- RF front-ends with complete band coverage (3.4 – 3.8 GHz FDD; 2.3-2.5 GHz TDD)
- High Power RF transmit module (up to 35 dBm)
- Two Low Noise receivers to support diversity in reception
- Broadband frequency agility (125 kHz), limited by the duplexer bandwidth (14 MHz) only
- Automatic compensation of IDU-ODU cable attenuation

*CPE Architecture.* The CPE is built around Intel® PRO/Wireless 5116 chip which implements MAC and PHY layers compliant to IEEE 802.16-2004. An high power (up to 27dBm) RF module guarantees outstanding radio performance.

In order to simplify the RF circuits, an Half-Frequency Division Duplex solution has been implemented. The greater complexity of the scheduling process deriving from that choice is well rewarded in terms of lower cost of the CPE.

The main features of the CPE are:

- Bridge (Layer 2) or Routed (Layer 3) operation
- DHCP Server and NAT (in routed mode)
- QOS support (incoming packets classification)
- 10/100 Ethernet Interface

### 2.8. *Redundancy*

Due to the high traffic capacity involved, protection from failures is supported for radio and Network Interface in the Base Station.

Automatic protection of the Network Interface and the Controller is provided at physical layer by means of a (1+1) redundancy of the CSU card. Automatic protection of the SMU and RF units is provided by means of a (N+1) configuration.

### *2.9. Synchronization*

The synchronization architecture in the Base Station allows a common reference-clock distribution to the SMU cards.

The reference clock can be selected between an external 10MHz source, e.g. a GPS receiver, or a high stability (2 ppm) local oscillator.

Inside each Radio Sector, the reference clock extracted by every CPE from the downlink stream will allow for a better performance of the demodulation process in the Base Station.

In order to achieve frame synchronization among adjacent cells, practically an obliged choice in TDD mode, a 1pps input connector is available on CU.

## 3. HOW THE SIEMENS SOLUTION FACES THE TECHNICAL CHALLENGES OF THE STANDARD

One of the main challenges deriving from the IEEE 802.16 standard is the required system flexibility in terms of physical layer robustness and adaptability to the transmission medium characteristics.

Most of the Users will be in non-line-of-sight (NLOS) condition; in such a condition the propagation will be multipath-based. The OFDM coding combined with the adaptive modulation and coding scheme is the best choice for facing this strongly variable propagation conditions.

The Siemens platform fulfils completely these requirements, having demonstrated in real Customer deployments the ability to face the strongly impaired propagation conditions by guaranteeing the network connectivity for "distant" Users, and to provide high bandwidth capacity for "near" Users at the same time.

For such a need an adaptive centralized data scheduling algorithm has been specifically developed to support the required Quality of Service. Even in case of impaired propagation conditions, the Base Station is able to cope with different modulation/coding schemes in the same radio Sector and to exploit the statistical multiplexing possibility of the multi-user shared medium.

To improve the performance of the physical layer, the Siemens platform provides a Diversity receiver in the Uplink direction, that can be configured for "Dual polarization diversity" or "Space diversity". The Diversity scheme has demonstrated an effective improvement in the Uplink performance, useful in balancing the often asymmetric link budged due to a low power/low cost CPE.

## REFERENCES

[1] IEEE Std 802.16$^{TM}$ -2004, "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems", October 2004
[2] IEEE 802.16.3c-01/29r4, "Channel Models for Fixed Wireless Applications", July 2001
[3] IETF Network Working Group, "RFC 2865: Remote Authentication Dial In User Service (RADIUS)", June 2000
[4] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, May/June 2004
[5] R. van Nee and R. Prasad, "OFDM for wireless multimedia communications", Artech House universal personal communication library, 2000