RTS/CTS mechanism with 802.11 for indoor location

J. Prieto[*], A. Bahillo[*], S. Mazuelas[*], J. Blas[*], P. Fernández[#], and R. M. Lorenzo[#]
[*]CEDETEL (Center of the Development of Telecommunications)
Edificio Solar. Parque Tecnológico de Boecillo. 47151. Boecillo (Valladolid). SPAIN
Email: jprieto@cedetel.es
[#]Department of Signal Theory and Communications and Telematic Engineering
University of Valladolid. Camino del Cementerio s/n. 47011. Valladolid. SPAIN
Email: patfer@tel.uva.es

***Abstract*—Trilateration techniques for position estimation use distances measurements in order to determine the unknown location of a mobile user. In this paper, a Time of Arrival (ToA) based method for estimating distance in an IEEE 802.11b network is presented. This method uses the RTS/CTS handshake and an external time counter for computing the Round Trip Time (RTT) and estimate the ToA.**

The system designed is tested in several real environments distinguishing line-of-sight (LOS) from non line-of-sight scenarios. By means of a linear regression of RTT measurements one meter accuracy is achieved for the LOS scenario.

***Keywords*—Distance estimation, IEEE 802.11, indoor location, Round Trip Time, Time of Arrival.**

I. INTRODUCTION

Most of the IEEE 802.11 location approaches correspond to radio-map based techniques, but they are not flexible because they present high variability due to environmental changes. Several indoor location techniques are based on the estimate of certain parameters taken from the RF signals that travel between the mobile user (MU) to locate and the fixed access points (AP) whose positions are known. Techniques based on the angle of arrival (AoA) require specialized antennas, some techniques based on received signal strength (RSS) require channel modeling, and several techniques based on time of arrival (ToA) need time synchronization between nodes.

In this paper, the performance of the IEEE 802.11 networks for indoor location based on ToA measurements is evaluated in terms of accuracy and complexity. To obtain accurate ToA estimations, round trip time (RTT) measurements have been used while avoiding the need for time synchronization between nodes. This method uses the common protection mechanism to fully reserve a shared medium in IEEE 802.11 WLANs, Request-To-Send (RTS) / Clear-To-Send (CTS) handshake, in order to assure that the RTT measurements are independent of the traffic load [1].

This research is partially supported by the Directorate General of Telecommunications of the Regional Ministry of Public Works from Castilla y León (Spain).

In [2], RTT measurements are taken to explore the degree of accuracy to which the propagation delay of WLAN packets can be measured using common commercial inexpensive equipment. In [3], a prototype is implemented in order to assess the validity and evaluate the performance of the RTT measuring technique.

Similarly to [3], in this paper, RTT measurements are carried out by implementing a counter as additional external circuit in the WLAN adapter. The counter is activated when the WLAN adapter sends the last bit of an RTS frame and deactivated when it receives a CTS response. Several series of measurements were taken in order to analyze their distribution in different line-of-sight (LOS) and non-LOS (NLOS) scenarios. In [3], distance is estimated using the average and the standard deviation of RTT measurements and subtracting the average at distance 0m. Moreover, in [3], a Gaussian distribution is fitted to the probability density function (PDF) of the distance estimation. However, in next sections, a method to estimate the distance from a linear regression is presented. And in contrast to [3], the analysis will allow to illustrate the lack of normality in the measurements.

Once distance is estimated and the position of the APs is supposed to be known, a trilateration technique can be used in order to survey the MU position. In this way, the power received from the APs is used to select which of them will be used to locate the MU, while RTT measurements, more strongly correlated with the distance than the power received, are used to estimate the distance between the MU and each AP.

The structure of the paper is as follows. The convenience of the use of the RTS/CTS mechanism is discussed in Section II where specific signals of the WLAN adapter will be described. Those signals are used by the hardware system to start and to stop the count. Afterwards, this contribution describes the design of the printed circuit board (PCB) used as a signal propagation time counter. The next two sections are about RTT measurements. The first one describes the different scenarios where time measurements have been taken while in Section IV the distribution of those measurements and the way distance is estimated from the RTT measurements are analyzed. Finally, a method for position estimation and NLOS mitigation is put forward, which will focus future essays on radiolocation.

II. TOA ESTIMATION

A. RTT measuring

In order to estimate the ToA, RTT measurements were taken at data link level from the IEEE 802.11 four-way handshaking RTS/CTS. When an RTS frame is sent by the MU a time counter is activated with the last bit, and it is stopped with the first bit of the corresponding CTS frame response coming from the AP. All measurements are taken in the MU, so this method avoids the synchronization between it and the AP. Moreover, there are two advantages of using the RTS/CTS mechanism. On one hand, the small and constant size of RTS/CTS frames will reduce and keep constant the AP processing time. On the other hand, the Short Inter-frame Space (SIFS) time, which is used for the highest priority transmissions like CTS responses, is independent of the traffic load, therefore AP processing time is supposed to be constant.

In [3], ToA is estimated by dividing the ΔRTT by two, where ΔRTT is obtained by subtracting the RTT at distance 0 m to the RTT at each distance. Once ToA is obtained, the distance between the MU and one AP is calculated by multiplying the ToA estimate by the speed of light in the media. However, in next sections, the efficiency of the sample mean in a linear regression will be evaluated as estimator of the distance, achieving an accuracy greater than the one obtained in [3].

As demonstrated in [4], the range resolution is directly related to the bandwidth of the transmitted signal by $\Delta r = \nu / 2BW$, being ν the speed of light in the media, and *BW* the bandwidth which is 22 MHz for an IEEE 802.11b WLAN. According to this, it is possible to achieve an accuracy of 6.8 m, nevertheless, as shown in Section IV, it will be improved by a linear regression model.

The main drawback of the time measuring method described at [2] is the low resolution of a computer clock. Normally, x86 PCs contain the 8253 or 8254 Programmable Interval Timer which perform timing and counting functions [5]. Usually, the timer use a 1.193.180 Hz signal as clock input giving a resolution of 838 ns, which makes impossible to achieve the aforementioned accuracy of 6.8 m. On the other hand, the aim of this work is to develop a measuring system independent of the device on which it is running. Thus, in this paper, the time counter is located at the WLAN adapter, and its clock is used as the time base.

The chipset specifications privacy hampered the choice of the WLAN adapter, making necessary to use one whose electronic performance was known. In [6], appropriate signals from within the Intersil HFA3863 baseband processor are used in order to measure the latency of ACK frames which makes possible to use the relative position with respect to an AP as the determining factor in granting network access to a potential MU. In [7], an implementation of the standard for synchronization IEEE 1588 working with Intersil HFA3861B signals is presented. And in [8], a WLAN location technique is proposed utilizing the Intersil chip HFA3860BIV. Thereby, an Intersil baseband processor was a widespread robust solution. The selected Cisco Aironet AIR-PCM340 IEEE 802.11b WLAN adapter contains the Intersil chip HFA3861B.

According to the HFA3861B pinout, three suitable signals (TX_RDY, MD_RDY and MCLK) and common ground were identified [9]. TX_RDY is an output to the external network processor indicating that the HFA3861B is ready to receive the data packet from the network processor over the TXD serial bus. When this signal turns off, all the data of the RTS frame have been sent. MD_RDY is an output signal to the network processor, which signals the start of data transfer over the RXD serial bus. MD_RDY goes active when the first bit of the CTS response is received. MCLK is the 44 MHz master clock for device. This is used internally to generate all other internal necessary clocks. TX_RDY and MD_RDY are used as timestamps of the RTS departure and the CTS arrival respectively, and the MCLK as the time base to measure the delay between both frames.

In [6], RX_PE is used instead of the signals mentioned. This is active when the receiver is configured to be operational, and otherwise it is in standby mode. Thus, RX_PE is activated with the last bit of the RTS frame and turned off with the last bit of the CTS frame, which supposes to add the AP transmission time to the RTT estimation. Thereby, RX_PE is not selected as it overestimates the RTT.

In case TX_RDY and MX_RDY were asynchronous, an external higher frequency clock would improve the time resolution. By visualizing one of those signals and the MCLK on an oscilloscope, and establishing TX_RDY or MD_RDY as external trigger, it was proved that the signals switch synchronously with the MCLK. The synchronism between MCLK and TX_RDY falling edge is corroborated in Fig.1. Therefore, the accuracy will not be improved although a higher clock frequency was used.

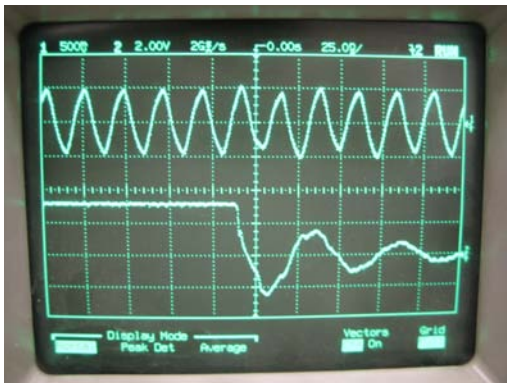


Figure 1. Synchronism between the MCLK (channel 1, upper line) and the TX_RDY falling edge (channel 2, lower line). The TX_RDY falling edge is configured as the external trigger.

In [2], the presence of measurement noise is assumed, and the sample mean of a Gaussian noise

distribution with a suitable strength is taken to enhance the resolution. For a normally distributed data set, 95% of the data observations are within 1.96 standard deviations of the mean. Thus, measurements out of this bound were discarded, and errors due to electronic noise or foreign frames were rejected.

To ensure that in a LOS scenario the RTT is only related with the distance and it is not affected by the AP processing time, the same process can be carried out by configuring the WLAN adapter in master mode, in order to check the AP processing time is constant. In that way, this time can be measured between the MD_RDY falling edge (RTS arrival) and the TX_RDY rising edge (CTS departure). However, as explained above, theoretically this time is supposed to be constant [1].

B. PCB design

The hardware system designed to measure RTT consists of a 16-bit clock cycle counter integrated into a Printed Circuit Board (PCB) which interacts between the WLAN adapter chipset and the PC parallel port. As illustrated in Fig.2, the 16-bit counter is made up of four serial 4-bit counters, which are activated and deactivated with the output of a previous stage composed by an XOR gate and a dual D-type Flip-Flop which handle the signals from the WLAN adapter. Nevertheless, if the counter system was integrated in the WLAN adapter, the only essential component would be the 16-bit counter.

The PCB is preceded by a security circuit to avoid damaging the parallel port by power surges coming from the PCB or by extracting more than the maximum output current from the parallel port [10]. The laptop activates the counters before sending the RTS frame and deactivates them after receiving the CTS frame. Therefore, once the counter is activated, wrong measurements will be obtained if a frame from other network arrives at the WLAN adapter before the CTS response. However, a method for discarding this values was presented in previous section.

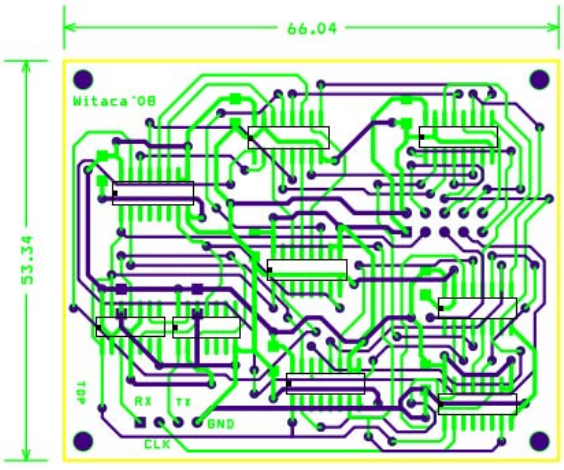


Figure 2. Printed Circuit Board used to measure the time between the IEEE 802.11 RTS/CTS handshake (dimensions in millimeters).

As the parallel port was selected to interact between a laptop and the PCB, it was not possible to read 16 bits and write 4 bits simultaneously, thus, three quadruple 2-input multiplexers were used. This is shown in Fig.2. After the RTS/CTS two-frame exchange is complete the laptop saves the state of the four 4-bit counters through the multiplexers.

With a working frequency of 44 MHz, it is necessary to implement several elements to keep the voltage constant and noise-free. With the aim to reduce the loop area, both for the supply and for the signal tracks, top and bottom planes were poured of copper, one attached to the power supply lead and the other attached to the ground. This will minimize the impedance of the return path [11]. Nevertheless, for better understanding, those copper planes were removed from the Fig.2.

Furthermore, one bypass capacitor was connected to each integrated circuit between its power pins to form a low pass filter which will prevent from high frequency disruptions.

III. EXPERIMENTAL SETUP

As mentioned previously, the MU consisted of an IEEE 802.11b WLAN adapter with the Intersil HFA3861B, plugged into a laptop through a PC CardBus extender which allowed the leads of the chip to be connected to the PCB.

Several tests were carried out in three different scenarios of the Higher Technical School of Telecommunications Engineering (University of Valladolid), analyzing the empirical distribution of the RTT measurements between the MU and an IEEE 802.11b/g AP in each of the scenarios. Three series of 5000 measurements were carried out for several distances until 40 m. The software used is an ANSI C code based on Linux-wireless-tools and on the Loss of Radio Connectivity (LORCON) library, which is a generic library for injecting IEEE 802.11 frames [12].

In two of the three scenarios, the MU and the AP were in LOS situation, while in the other one, the MU and the AP were separated by a wall 20 cm width next to the AP, along a corridor of the School, in the following NLOS. The LOS scenarios were the same corridor of the School (without the wall), with some metallic doors and objects, and a few people, in the following HTS; and the outside of the School with a few lampposts, trees and people, in the following EXT. It should be notice that several IEEE 802.11b/g networks were configured at the School to provide Internet access to many wireless devices, which will cause noise to be introduced in the distance estimation. In the three scenarios, the MU and the AP were placed on a cardboard box 1 m high in order to prevent the Fresnel zone.

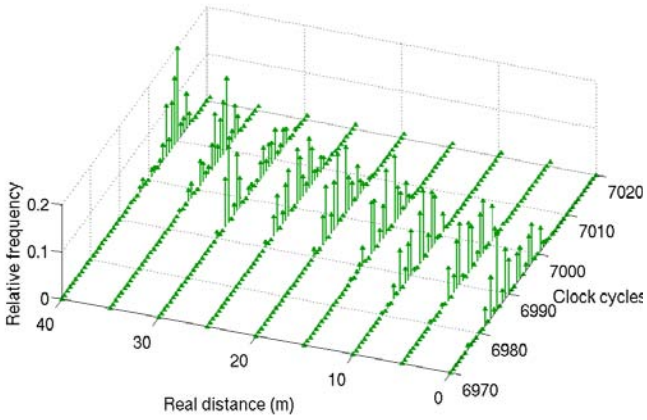
In next section, measurements in NLOS and HTS scenarios are compared in order to analyzed the distribution of the observations for the same conditions, being the only difference the presence of the wall next to the AP. And the results obtained in EXT are used to estimate the distance avoiding the

influence of other elements like signal reflections on the walls.

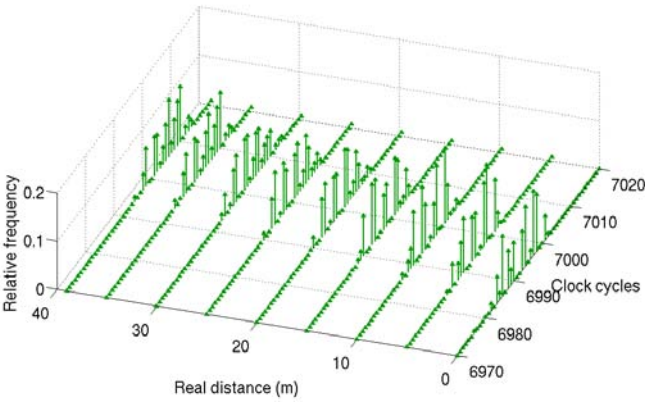
IV. EXPERIMENTAL RESULTS

A. RTT measurements

In Fig.3(a), the distribution of the number of clock cycles measured by the designed system in the LOS scenario (HTS) is shown, every five meters from 0 m until 40 m. It is appreciated how the number of clock cycles grows with distance. In Fig.3(b), the results of the campaign conducted in the NLOS scenario are shown. In this case, measurements were taken at the same distances as the previous scenario, apart from 40 m distance, which was carried out at 39 m due to the features of the corridor. Regarding the real distance, a similar behaviour of the number of clock cycles is observed. However, the peak of the distribution goes towards higher values which was expected as there are a major number of reflections in the NLOS scenario.



(a) LOS scenario



(b) NLOS scenario

Figure 3. RTT measurements distribution in (a) LOS situation and (b) NLOS situation.

As mentioned above, in [2] a Gaussian distribution is assumed for the errors. In [3], the statistical model proposed is a Gaussian distribution as the PDF of the distance estimations. In order to verify the assumption of normality, a nonparametric method is carried out as nothing is known about the parameters of the variable of interest concerning its distribution. The Kolmogorov-Smirnov (KS) one-sample test for normality is based on the maximum difference between the sample cumulative distribution and the hypothesized cumulative distribution.

As the mean and the standard deviation of the hypothesized normal distribution are not known a-priori, those parameters have to be estimated from the actual data. In that case, Lilliefors probabilities should be used in determining whether the KS difference statistic is significant [13]. As shown in Table I, the value of this statistic (D) is greater than the corresponding critical value (C), being the p-value smaller than 0.001, for each distance and for the two presented scenarios. Therefore, the assumption of normality might not be accepted for any distance and any scenario at significant level 0.05. Although the test is relatively weak the p-values obtained are small enough to assure the lack of normality.

Table I
KS TEST FOR LOS AND NLOS SCENARIOS

		0m	5m	10m	15m	20m	25m	30m	35m	40m*
LOS	D	0.145	0.147	0.142	0.149	0.145	0.110	0.211	0.137	0.166
	C	0.014	0.014	0.014	0.014	0.014	0.014	0.014	0.014	0.014
NLOS	D	0.144	0.178	0.143	0.169	0.138	0.118	0.106	0.139	0.103
	C	0.013	0.013	0.014	0.014	0.014	0.014	0.014	0.014	0.014

*39 for NLOS scenario

B. Distance estimation

In Fig.4 is illustrated the real distance as a function of the time measurements (in clock cycles). The relative frequency of each dot is represented by its color according to the colorbar shown on the right of the figure. Measurements were taken every two meters from 0 m to 20 m, and every 5 m until 40 m.

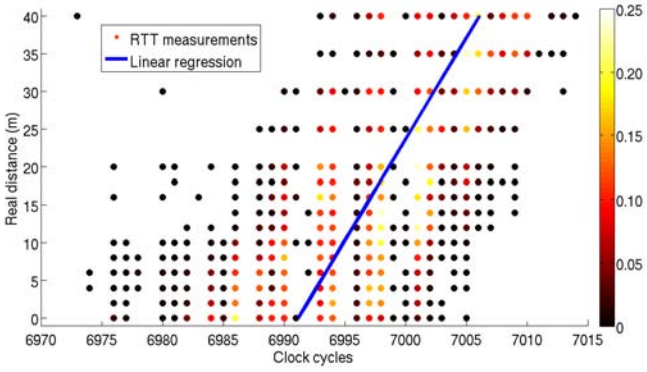


Figure 4. Distribution of the RTT measurements in the outdoor, and linear regression for estimating the distance from RTT measurements.

Two linear regressions were made in order to estimate the distance from RTT measurements. One regression was made taking the sample mean of the

measurements as estimator, and another taking all the samples. The same coefficients were obtained by means of the two methods, thus, only one regression line is represented. As shown in Fig.4, this line matches with the zone where the dots indicate a higher frequency. The accuracy achieved by this regression is around 1 meter without considering previous position estimations.

C. Indoor location

In this paper, the purpose of developing a ToA-based hardware system for distance estimation is to use it for indoor location. Trilateration techniques manage distance measurements to survey the spacial coordinates of unknown positions [14]. The practical indoor trilateration is as follows. The MU to be located measures on average, the power of the beacons transmitted by each AP inside its coverage area, which positions are supposed known. The more power on average received, the more proximity to this AP the terminal is located. As a consequence, theses APs will be used to infer the MU position. The developed software allows the adapter to change easily the AP to which it is connected. The MU uses the flight duration of the RTS/CTS frames to measure the RTT between itself and each AP. Finally, to determine the MU position in the area, the trilateration technique is used.

In this way, the power received from the APs is used to select the APs which will be used to locate the MU while RTT measurements, which are correlated with the distances more strongly than the power received, are used to estimate the distance between the MU and each AP.

V. CONCLUSIONS

This paper evaluates the convenience of implementing a small external hardware subsystem for measuring RTT and estimating the distance between a MU and an AP whose position is known. The experimental results showed that estimations are not characterized by a Gaussian distribution as it was assumed in [2] and fit in [3].

Afterwards, a linear regression was made for the LOS scenario, achieving an accuracy of around 1 m in distance estimation. However, the existence of NLOS propagation paths has been considered the main drawback to achieved high precision in the positioning due to unpredictable errors introduced in the RTT estimations. In order to correct the measurements from NLOS, in [15] is proposed a technique called prior NLOS measurements correction which should be conducted in a previous stage to the position process.

Next step, will consist of estimating the position from the RTT measurements to at least three APs. Furthermore, channel characterization, tracking techniques and optimum geometric distribution of the APs should be used in order to improve the accuracy of 1 m achieved.

REFERENCES

[1] "IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 8: Medium Access Control (MAC) Quality of Service (QoS) Enhancements", IEEE Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) IEEE Std 802.11e–2005, Nov. 2005.

[2] A. Günter and C. Hoene, "Measuring Round Trip Times to Determine the Distance between WLAN Nodes", Telecommunications Network Group, Technical Report, Dec. 2004.

[3] M. Ciurana, F. Barcelo-Arroyo and F. Izquierdo, "A Ranging System with IEEE 802.11 Data Frames", Proc. of the Annual International Conf. of the IEEE RWS, Jan. 2007.

[4] V. C. Chen and H. Ling, "Time-Frequency Transforms for Radar Imaging and Signal Analysis", Norwood, MA, USA: Artech House, 2002.

[5] Data Sheet, Intel 82C54 CHMOS Programmable Interval Timer, Oct. 1994.

[6] J. D. Morrison, "IEEE 802.11 Wireless Local Area Network Security Through Location Authentication", Naval Postgraduate School Monterey, California, Thesis, Sep. 2002.

[7] T. Cooklev, J. C. Eidson and A. Pakdaman, "An Implementation of IEEE 1588 Over IEEE 802.11b for Synchronization of Wireless Local Area Network Nodes ", IEEE Transactions on Instrumentation and Measurement, vol. 56, No. 5, Oct. 2007.

[8] F. Izquierdo, "Wireless LAN location technique based on Round-Trip-Time measurements", Final Year Project, Barcelona, Spain, Jun. 2005.

[9] Data Sheet, Intersil HFA3861B Wireless LAN Medium Access Controller, Feb. 2002.

[10] D. V. Grade, "Programming the Parallel Port. Interfacing the PC for Data Acquisition and Process Control", Lawrence, USA, Jan. 1998.

[11] J. R. Barnes, "Robust Electronic Design Reference Book", Vol. I, Mar. 2004.

[12] J. Wright and M. Kershaw, "Extensible 802.11 packet Flinging", Annual East Conf. ShmooCon, Washington DC 2007.

[13] H. Lilliefors, "On the Kolmogorov-Smirnov test for normality with mean and variance unknown", Journal of the American Statistical Association, Vol. 62. pp. 399-402, 1967.

[14] D. J. Torrieri, "Statistical theory of passive location systems," IEEE Transactions on Aerospace and Electronic Systems, vol. 20, no. 2, pp. 183-198, 1984.

[15] S. Mazuelas, F. A. Lago, J. Blas, A. Bahillo, P. Fernández, R. M. Lorenzo a and E. J. Abril, "Prior NLOS Measurements Correction for Positioning in Cellular Wireless Networks", IEEE Trans. Vehicular Technology (accepted for publication), Sep. 2008.

Javier Prieto received the Telecommunication Engineer degree from the University of Valladolid, Spain, in 2008, where he is currently studying Marketing Research and Techniques and working towards the Ph.D. degree in the Department of Signal Theory and Communications and Telematics Engineering.

He joined CEDETEL (Center for the Development of Telecommunications in Castilla y León) in 2007. His research interests include radiolocation techniques for indoor and outdoor communications.

Alfonso Bahillo received the Telecommunication Engineer degree from the University of Valladolid, Spain in 2006, where he is currently working toward the Ph.D. degree in the Department of Signal Theory and Communications and Telematics Engineering.

He joined CEDETEL (Center for the Development of Telecommunications in Castilla y León) in 2006. His research interests include numerical methods in electromagnetics, radio propagation modeling and radiolocation techniques for indoor and outdoor communications.

Santiago Mazuelas received his Mathematics and Telecommunication Engineer degrees from the University of Valladolid, Spain, in 2002 and 2007, respectively.

Since 2006 he has worked as Researcher in CEDETEL (Center for the Development of Telecommunications). He is currently working toward the Ph.D. degrees in Mathematics and Telecommunications. His research interests include radiolocation technologies and mathematics.

Mr. Mazuelas has received the young scientists prize for the best communication in the Union Radio-Scientifique Internationale (URSI) XXII Simposium (Spain).

Juan Blas obtained his Telecommunication Engineer degree from the University of Valladolid, Spain, in 2001, where he received his Ph.D. Degree in 2008.

He joined CEDETEL (Center for the Development of Telecommunications in Castilla y León) in 2006. His research interests include radio wave propagation and the development of numerical models to evaluate human exposure to RF sources.

Patricia Fernandez received the Telecommunication Engineer degree from Universidad Politécnica de Cataluña, Barcelona, Spain, in 1997 and the Ph.D . degree in 2004 from University of Valladolid.

Since 1999 she has worked as a Junior Lecturer at the University of Valladolid. Her current research interests are communication systems and networks, electromagnetic characterization and radiolocation.

Dr. Fernández is the author of more than 40 papers in international journals and conferences.

Ruben M. Lorenzo received his Telecommunication Engineer and PhD degrees from the University of Valladolid, Spain, in 1996 and 1999, respectively.

From 1996 to 2000, he was a Junior Lecturer at the University of Valladolid, and joined the Optical Communications Group. Since 2000, he has been a Lecturer. He is currently the Head of the Faculty of Telecommunication Engineering at University of Valladolid and Research Director of CEDETEL (Center for the Development of Telecommunications in Castilla y León). His main research topics include communication systems and networks, electromagnetic characterization and radiolocation.