A ranging system with IEEE 802.11 data frames

M.Ciurana, F.Barcelo-Arroyo and F.Izquierdo
Department of Telematic Engineering
Universidad Politècnica de Catalunya, Barcelona, Spain

***Abstract*—Accurate indoor positioning with minimum dedicated infrastructure is required for certain critical applications such as emergency rescue, fire brigades or incident management. This paper presents an innovative TOA-based ranging technique for IEEE 802.11 networks, which is one of the essential steps towards achieving the desired location technique. Our approach is based on *RTT* measurements using standard IEEE 802.11 link-layer frames. Due to the noise in the measurements, accurate statistical post-processing is required. Ranging results obtained using the proposed technique show an encouraging achievable accuracy with an error of less than one meter.**

***Index Terms*—IEEE 802.11, ranging, *RTT*, *TOA*, WLAN**

I. Introduction: motivation and goals

SOME critical applications and services based on indoor localization—such as emergency rescue, fire brigades or incident management—need an easily deployable positioning system able to provide high-accuracy positioning (i.e. an error of close to 1 m) in medium and deep indoor environments. Since global (i.e. GPS) and wide-area (i.e. cellular networks) location systems remain inefficient indoors, alternative positioning technologies are required. Researchers are taking up the challenge of creating an indoor location system capable of providing accurate positioning using the existing WLAN infrastructure with minor changes (i.e. taking advantage of the wide deployment of the IEEE 802.11 standard), thus avoiding the need for synchronization between access points (e.g. as in TDOA-based systems) or long system pre-calibrations (e.g. of a fingerprinting database [1]).

Following this trend, the research presented in this paper is aimed at designing a system to locate WLAN terminals in indoor environments based on Time of Arrival (*TOA*) and trilateration ([2]). In such a system, estimations of the distance between the MT and several APs must be obtained so that a trilateration algorithm may be applied to calculate the MT's position using the estimated distances and the APs' known positions. This paper presents a novel distance-estimation technique that uses IEEE 802.11 standard frames to calculate *TOA*. It involves minimum modifications in the terminal and provides the targeted ranging accuracy. Since a decentralized architecture is preferred in order to maximize system scalability and user privacy, the ranging capabilities (and positioning capabilities, in a subsequent step) are assumed to be located in the MT, but this hypothesis can be easily generalized.

II. Description of the method

A. Distance-estimation approach

The distance between two wireless nodes can be estimated using a TOA-based or Received Signal Strength (RSS) method. Since *TOA* is more stable and there is a stronger correlation with distance than RSS, it is usually more accurate. The ranging technique presented here is based on a *TOA* estimation. The distance a between the MT and one Access Point (AP) can be obtained by multiplying the *TOA* estimate (i.e. propagation delay of the signal) by the speed of light (c):

$$a = c \cdot t_p = c \cdot TOA . \quad (1)$$

In order to avoid the need for time synchronization between the WLAN nodes, which would entail a major increase in the complexity of system deployment and cost, *TOA* is obtained by performing round-trip time (*RTT*) measurements from the MT to a fixed AP. The *RTT* is the time the signal spends traveling from a transmitter to a receiver and back again to the transmitter. The *TOA* estimate for a distance a is then obtained by halving the ΔRTT, which corresponds to the pure propagation portion of the *RTT*. Hence, Eq. (1) can be rewritten as:

$$a = c \cdot \left(\frac{\Delta RTT}{2} \right). \quad (2)$$

In terms of accuracy, *RTT* measurements should ideally be performed at the physical level using a delta impulse and the proper signal-processing functionality, but such a solution would require specific, expensive hardware and is unfeasible given our design constraints. Our approach takes advantage of the existing IEEE 802.11 communications network infrastructure to achieve high ranging accuracy ([3]), so IEEE 802.11 standard frames are used to measure the *RTT*. The selected frames were the link-layer data and ACK frames. The *RTT* therefore corresponds to the time that elapsed between sending a link-layer data frame to the AP and the consequent reception of the link-layer ACK in the MT, as shown in Fig. 1. Other link-layer frames would also be suitable.

Fig. 1 shows that an *RTT* measurement at a distance a greater than zero includes the propagation and processing times:

$$RTT_a = t_{p\_data\_frame} + t_{proc\_data\_frame} + t_{p\_ACK} . \quad (3)$$

Given that the propagation time of the signal is the same for the data and ACK frames, Eq. (3) can be rewritten as:

$$RTT_a = 2 \cdot t_p + t_{proc\_data\_frame} . \quad (4)$$

1-4244-0445-2/07/$20.00 ©2007 IEEE

The ΔRTT corresponding to a distance a greater than zero is obtained by subtracting the MAC processing time of the data frame ($t_{proc\_data\_frame}$) from the RTT at this distance a (RTT_a), in order to isolate the time that the signal

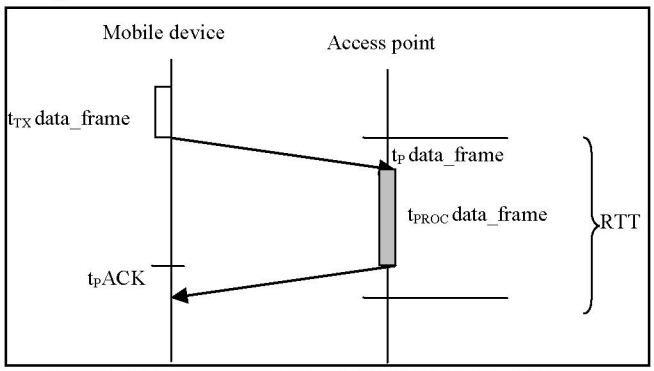

Figure 1. RTT measurement using IEEE 802.11 data/ACK frames.

spends propagating through the air. The processing time corresponds to the RTT when the transmitter and receiver are at distance zero, because the propagation time in such situations is null:

$$RTT_0 = t_{proc\_data\_frame}. \quad (5)$$

Hence, the ΔRTT can be obtained as follows:

$$\Delta RTT = RTT_a - RTT_0. \quad (6)$$

The distance formula, assuming a time counter at frequency f_{CLK} to count the RTT, can then be rewritten as:

$$a = c \cdot \left(\frac{RTT_a - RTT_0}{2} \right) \cdot \left(\frac{1}{f_{CLK}} \right). \quad (7)$$

B. *Mechanism for RTT measurement*

Nowadays, neither the IEEE 802.11 standard by itself nor the WLAN chipset manufacturers provide highly accurate timestamps in packet transmission and reception that would make it feasible to perform accurate RTT measurements by means of a pure software solution. However, high time resolution is necessary due to the high signal-propagation speed. In [4], a method for estimating the TOA between WLAN nodes without using additional hardware was presented: the authors collected IEEE 802.11 packet timestamps at a resolution of 1µs using *tcpdump* software and an additional monitoring node for taking RTT measurements. The error rate—of 8 meters—was poor compared to the 1 m error targeted in this paper. In order to overcome these limitations in a standard timestamp resolution, we decided to use the available WLAN card clock at 44 MHz as the time counter, so a noticeably enhanced resolution of 22 ns was achieved.

Furthermore, the RTT measurement mechanism was designed by taking into account the following two significant issues.

1. Measurements are taken at the lowest possible communications layer in order to avoid counting major additional delays due to inter-layer interfacing (e.g. frame encoding and decoding times).

2. Measurements are taken as close as possible to the WLAN hardware level in order to avoid delays due to WLAN card firmware/WLAN driver communication or operating system intermediation (e.g. interrupt latencies, communications stack processing, etc.).

Our solution was to directly extract MAC signals from the WLAN card chipset that indicated the transmission of the last bit and the reception of the first bit of a MAC frame, so that they could be used as triggers to start and stop the RTT count. This involved implementing a simple hardware module whose inputs are the aforementioned triggers and the clock signal from the WLAN card, and which provides output to the MT—through the parallel port—in the form of the RTT figure in units of 44 MHz clock rising edges. The basic RTT measurement system was completed with a software module in the MT that sends an ICMP Ping to the AP—in order to induce the transmission of the link-layer data frame—and stores the RTT measurement figure once the ACK has been received. Fig. 2 shows the implementation of the ranging platform described here, in which the MT is a laptop PC.

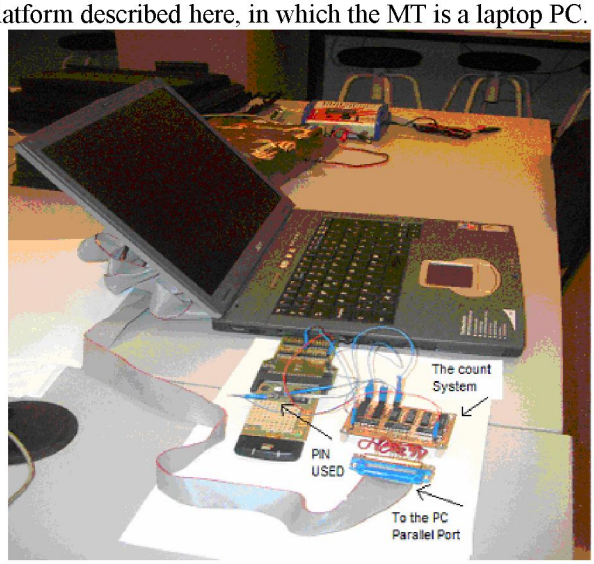

Figure 2. Developed ranging platform.

C. *Statistical processing*

We expected that the RTT measurements carried out by our ranging platform would not be totally stable due to several sources of randomness (listed below), most of which are related to the ranging measurement system:

- Discrete time quantification when using the 44 MHz clock, which can lead to distance errors of 7 m.
- Delays due to the WLAN hardware electronics in the MT and the AP.
- Delays due to the additional hardware counter module in the MT.
- Drift of the 44 MHz WLAN card clock in the MT during measurement.
- Relative drift between the clocks managing MAC processing in the MT and the AP.
- The inherent characteristics of the indoor wireless radio channel ([5]), including multipath.

The experiments conducted corroborated this premise because RTT measurements show time variability (see Section

III). Thus, the *RTT* is treated as a random variable and therefore ΔRTT is also a random variable obtained by subtracting two random variables (Eq. (6)).

Given this random behavior, several measurements are required when estimating an *RTT*, regardless of the distance between the MT and the AP. Therefore, we must choose a proper statistical estimator (average, half range, mode, etc.) to characterize the collected set of *RTT* samples in order to mitigate the impact of the different *RTT* noise components as much as possible. According to Eq. (6), there are two statistical alternatives for estimating ΔRTT at a distance a, both of which require a set of *RTT* measurements at distance 0 between the MT and the AP (which can be understood as a pre-calibration of the AP's processing time). In Section III, we explore and evaluate both in order to select the one that provides higher ranging accuracy.

1) Method A

First, estimators for the RTT_a and RTT_0 are separately obtained and subtracted to obtain the ΔRTT. Two approaches are presented: a) using the same estimator for both the RTT_a and RTT_0 and b) using a different estimator for each magnitude.

2) Method B

Samples of the random variable ΔRTT are obtained by subtracting the *RTT* measurements at distances a and 0, and finally a proper estimator is applied over them. Thus, the estimator is obtained over propagation time samples. The ΔRTT samples are obtained by taking each sample of the *RTT* series at distance a and subtracting a randomly selected sample of the *RTT* series at distance 0.

III. Experimental Results

Measurements were carried out indoors using the ranging platform at real distances ranging from 0 to 30 m at intervals of 3 m in a line-of-sight (LOS) situation between the platform and the AP. Both the MT and the AP were placed 1.5 m off the ground in order to preserve the Fresnel zone. For each distance, series of 1000 *RTTs* were collected. These *RTT* series were empirical distributions and were used to estimate the ΔRTT (and therefore the distance) and thus to make a comparative evaluation.

Fig. 3 shows the *RTT* empirical histograms of the 1000 *RTT* measurements obtained for 0, 6, 12, 18, 24 and 30 m. In order to obtain a clean representation, other distances have not been included. The results are qualitatively consistent because they shift to the right as the actual distance increases, with approximately constant separation between consecutive distributions. A quantitative analysis is performed below through two evaluations of the methods proposed. The *RTT* has a high time variability. For example, at 12 m, *RTT* figures lie between 6809 to 6821 44 MHz clock cycles, which means a wide variation range of 40 m in terms of distance.

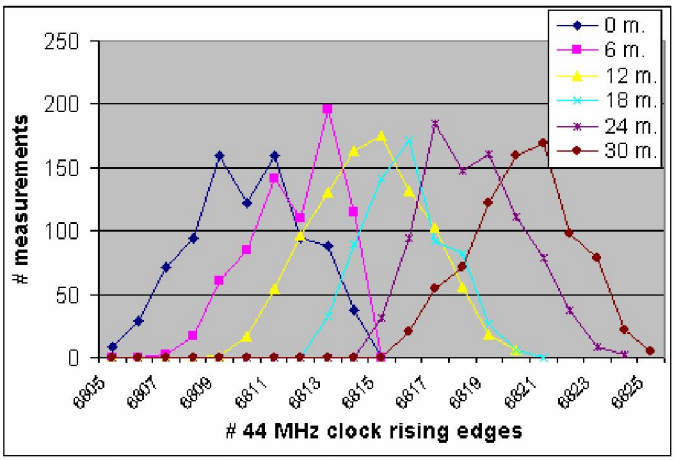

Figure 3. *RTT* histograms for 0, 6, 12, 18, 24 and 30 m.

A. Evaluation of Method A

This method is evaluated considering the following statistical estimators for the random variable *RTT*: average (η), half range, mode, minimum value, and average minus n times the standard deviation ($\eta - n \cdot \sigma$). As an estimator, the minimum is based on the assumption that the first frames to arrive are the most representative of the actual distance (i.e. they arrive through the shortest direct path). The $\eta - n \cdot \sigma$ algorithm was also considered for the same reason.

RTT estimations were performed using these algorithms, fed with the *RTT* series from the measurement campaign. Therefore, ΔRTT and the distance estimate were obtained using Eq. (7). Table I shows the performance of each estimator.

Table I. Ranging errors with the first approach of Method A.

Estimator	Average error (%)	Average error (m)
Average value (η)	40.21	2.82 m
Half-range value	59.80	4.43 m
Mode value	52.07	2.86 m
Minimum	30.20	2.72 m
η-σ	41.00	2.81 m
η-2σ	41.80	2.80 m
η-3σ	42.60	2.79 m

All the distance estimates obtained are greater than their actual corresponding distance, regardless of the *RTT* estimator used. We therefore decided to exploit the fact that the RTT_0 purely represents MAC processing while the RTT_a contains propagation time. The average is expected to be a good statistical estimator for a random variable corresponding to a processing time. For radio signal propagation time, an estimator that provides below-average figures is expected to be the most suitable because the lowest measurements obtained are highly relevant. Based on this idea, we also tested the distance-estimation accuracy provided by Method A using several *RTT* estimators at distances greater than zero (RTT_a) while using η for RTT_0 (η_0). The estimator $\eta - (\sigma/3)$ provided the best accuracy, so the ΔRTT expression according to Eq. (6) was ultimately:

$$\Delta RTT = \left(\eta_a - \frac{\sigma_a}{3} \right) - \eta_0 . \quad (8)$$

In practice, η_0 is 6810.28 44MHz clock cycles. Table II shows the ranging results obtained from Eq. (8). The average of the resulting absolute distance-estimation errors, taking into account all tested distances, is 0.81 m. The ranging accuracy is significantly better than that shown in Table I. The error provided by η as an estimator increases with distance. When estimating distance using Eq. (8), the absolute error remains stable because the standard deviation also increases with distance and compensates for the behavior of η.

Table II. Ranging results with the second approach of Method A.

Dist (m)	RTT standard deviation	RTT_a est. $\eta - (\sigma/3)$	Distance est. Eq (8)	Abs. error (m.)	Rel. error (%)
3	2.03	6811.05	2.62	0.37	12.47
6	2.12	6811.58	4.45	1.54	25.80
9	2.23	6812.71	8.28	0.71	7.89
12	2.39	6813.66	11.52	0.47	3.93
15	2.33	6814.35	13.88	1.11	7.44
18	2.33	6815.38	17.37	0.62	3.45
21	2.35	6816.73	21.96	0.96	4.58
24	2.43	6817.68	25.21	1.21	5.06
27	2.41	6818.37	27.54	0.54	2.02
30	2.53	6819.25	30.55	0.55	1.83

B. *Evaluation of Method B*

After subtracting the empirical distributions of RTT_a and RTT_0, the empirical distribution for ΔRTT is obtained. Fig. 5 depicts this distribution together with the normal fits for distances of 18 and 27 m.

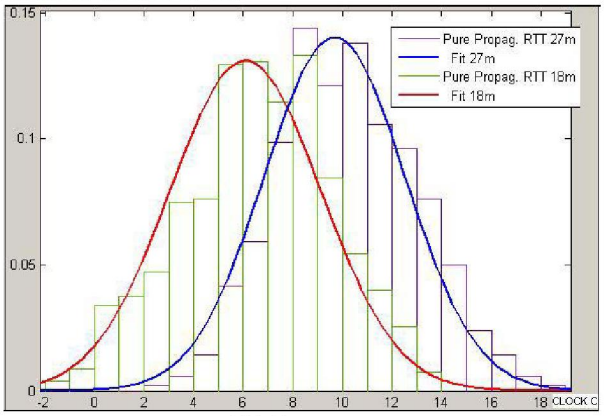

Figure 5. ΔRTT pdf for 18 and 27 m.

Several statistical estimators (average (η), half range, mode, minimum n value, and average minus n times the standard deviation ($\eta - n \cdot \sigma$)) were applied over these series of ΔRTT samples and then the estimated distance was calculated. The average was the best estimator. The estimator $\eta - n \cdot \sigma$ did not provide good results with reasonable n figures because the σ (standard deviation of a set of ΔRTT samples) figures were around 3 clock cycles and η (average of a set of ΔRTT samples) was between 1 and 10, so the resulting $\eta - n \cdot \sigma$ values were too small and hence yielded a high ranging error. Table III shows the results obtained with the estimator η. The average of the resulting absolute distance-estimation errors, taking into account all tested distances, is 2.63 m.

Table III. Ranging results with Method B.

Actual distance (m)	Distance estimate with Method B using η	Abs. error (m.)	Rel. error (%)
3	3.26	0.26	8.96
6	6.84	0.84	14.06
9	10.58	1.58	17.66
12	14.87	2.87	23.99
15	17.19	2.19	14.63
18	20.53	2.53	14.06
21	23.76	2.76	13.16
24	27.37	3.41	14.20
27	32.51	5.51	20.43
30	34.22	4.32	14.40

IV. Conclusions

In this study, we proposed and evaluated several *TOA*-based approaches for estimating distances in WLAN networks using standard data frames at the IEEE 802.11 MAC layer and a counter module with the WLAN card clock. Using different estimators for the *RTT* at an unknown distance and the *RTT* at a distance of zero gives ranging errors of under 1 m. This proves that time stamping of IEEE 802.11 packets using the available clock in the WLAN card would suffice to achieve accurate ranging capabilities. The results of this research can be applied to indoor locations and may give rise to major benefits because low-cost, high-accuracy location systems that are flexible and easily deployable would be feasible.

Acknowledgment

This research was funded by the EC under the Sixth FP IST LIAISON Integrated Project and by the Spanish Government and FEDER through Plan Nacional de I+D (TEC2006-09466/TCM).

References

[1] M. Youssef, "Horus: a WLAN-based indoor location determination system," *Department of Computer Science, University of Maryland*, 2004.

[2] W. Murphy and W. Hereman, "Determination of a position in three dimensions using trilateration and approximate distances," *Colorado School of Mines*, Golden, CO. Tech. report MCS-95-07, 1995.

[3] X. Li; K. Pahlavan, M. Latva-aho, M. Ylianttila, "Comparison of indoor geolocation methods in DSSS and OFDM wireless LAN systems," *IEEE Vehicular Technology Conference*, Volume 6, 24-28, pp. 3015-3020, Sept. 2000.

[4] A.Günther, C. Hoene, "Measuring round trip times to determine the distance between WLAN nodes," *Networking*, pp. 768-779, 2005.

[5] H. Hashemi, "The indoor radio propagation channel," *Proceedings of the IEEE*, Vol. 81, No.7, pp. 943-968, July 1993.