This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

A ranging method with IEEE 802.11 data frames for indoor localization

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

***Abstract*—IEEE 802.11 networks constitute a suitable infrastructure for accurate indoor positioning. However, existing approaches based on fingerprinting present drawbacks that make them not suitable for most of applications. This paper presents an innovative TOA-based ranging technique over IEEE 802.11 networks intended to be the essential step of an indoor location system. This approach is based on round trip time measurements using standard IEEE 802.11 link layer frames and a statistical post-processing to mitigate the noise of the measurements. A prototype has been implemented in order to assess the validity and evaluate the performance of the proposed technique. First results show ranging accuracies of less than one meter of error in LOS situations.**

***Index Terms*—distance estimation, IEEE 802.11, indoor location, ranging, *RTT*, *TOA*, WiFi, WLAN**

I. INTRODUCTION: MOTIVATION AND GOALS

WIDE area positioning systems (e.g. GPS or cellular-based systems) do not work correctly in deep indoor environments. This fact presents a serious problem for location-based applications and services intended to work ubiquitously. Several different location techniques specifically designed for indoors have been proposed over the last years as possible solutions to this problematic. Some of those proposals entail the need for a dedicated infrastructure for positioning -based on RFID ([1],[2]), ultrasound ([3]) or even hybrid Bluetooth-IR techniques ([4])- but their main drawback is their complex and costly deployment. Recently, a growing interest of the scientific community in techniques that rely on IEEE 802.11 local area networks has been appreciated, since this type of communications infrastructure is being deployed in most of buildings and hence allows the design of flexible and low-cost positioning systems. However, currently available WiFi-based approaches are not mature enough and present noticeable drawbacks in terms of accuracy, availability, flexibility or time of deployment.

Most of the IEEE 802.11 location approaches correspond to radio-map based –also called fingerprinting- techniques, which are able to provide good positioning accuracy but entail a complex offline training phase to construct the radio-map and present high variability to environmental (i.e. furniture) changes. They can be divided in deterministic and probabilistic ones. The most widely known system from the first group is the Radar system ([5]), based on empirical signal strength measurements as well as a simple yet effective signal propagation model. Its average resolution is in the range of 3 meters. Enhancements to this system have been proposed based on Continuous User Tracking and the use of Viterbi-like Algorithms ([6]). They can increase the accuracy up to 2.37 m. In the probabilistic systems, the Horus system can obtain results with over 90% accuracy within 2.13 meters with very low computational requirements ([7]). It has been compared with the Radar system and the tests carried out show that Horus outperforms Radar. Some other systems are the Nibble location system, which uses a Bayesian network to infer a user location. This system can find with precision the room where the mobile device is located, being the rooms of dimensions of 2 x 4 m ([8]). Tracking assistant techniques that use topological knowledge to assist the position determination can locate mobile devices with a 2 m accuracy with a probability of 90% and moving mobile devices with a 5 m accuracy with 90% probability as well ([9]). Besides, Bayesian-Hidden Markov Models techniques can achieve an accuracy of 1.5 m with a 70 % probability ([10]). Regarding the commercial systems, the main solution offered to date is the Ekahau Positioning Engine ([11]).

The other proposals belong to the time-based group, mainly based on Time Of Arrival (*TOA*) or Time Difference Of Arrival (TDOA) ([12]), in which distance estimations –that is ranging- from the terminal to several Access Points (APs) are typically needed. This paper presents a new *TOA*-based ranging technique that constitutes the essential step to achieve the indoor positioning system. TDOA has been discarded due to the need of synchronization between nodes, and the possibility of measurements based on Received Signal Strength Indicator (RSSI) has not been taken into account because the achievable accuracy is quite low. The proposed method overcomes the limitations of the existing ranging approaches, using standard IEEE 802.11 frames and the minimum modifications in the terminal to obtain accurate *TOA* –and hence distance- estimations, while avoiding the need of synchronization between nodes.

In [13] a ranging in IEEE 802.11 is presented without the requirement of initial synchronization between transmitters and receivers. Ranging is achieved by using a high precision timer in order to measure TDOA from two GRP (Geolocation Reference Point). The authors also propose to take advantage of the IEEE 802.11 data link frames for measuring *TOA*, but they do not give more insight into this matter. In [14], a system which can estimate *TOA* using IEEE 802.11 link layer

frames is proposed, but the RTS (Request-to-Send)/CTS (Clear-to-Send) mechanism is required. Their ranging technique relies on internal delay calibration both at the transmitter and receiver in order to correct the round trip time (*RTT*). Our approach avoids using the RTS and CTS control frames since in most WiFi networks they are not enabled. In [15], a method to estimate *TOA* between WLAN nodes without using extra hardware is presented, but the achieved accuracy (error of 8 meters) is not enough for some safety applications.

The paper is organized as follows. In Section II the method to estimate the distances is described, including the principles of the mechanism, a brief explanation of the implementation and the specific statistical processing used as final algorithm. Section III presents the distance estimation statistical model obtained from an exhaustive measurement campaign. Section IV presents an evaluation of the main application of the presented ranging technique, which corresponds to indoor positioning through trilateration. Finally, in Section V conclusions are provided.

II. DESCRIPTION OF THE METHOD

A. Distance estimation approach

As stated above, the ranging technique presented here is based on *TOA* estimation, so that the distance *a* between the mobile terminal (MT) and one AP is obtained by multiplying the *TOA* estimate by the speed of light (*c*):

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

TOA is obtained by performing *RTT* measurements from the MT to a fixed AP in order to avoid the need for time synchronization between the WLAN nodes, fact that would increase the complexity and cost of deployment of the system. The *RTT* is the time spent by a signal or message in traveling from a transmitter to a receiver and back again to the transmitter. Since our approach aims to take the maximum advantage of the existing IEEE 802.11 communications network infrastructure to accurately estimate the distances, IEEE 802.11 standard frames are used for measuring *RTT*, specifically the data and ACK MAC frames (see [16] for more details). This could be performed using other link layer frames, but for instance the RTS-CTS mechanism is not enabled in most of the IEEE 802.11 networks so their use would limit the deployment of the technique.

From Figure 1 and taking into account that the propagation times for the data and ACK frames are supposed to be the same, it can be stated that:

$$TOA = \frac{RTT_a - t_{proc\_data\_frame}}{2}, \quad (2)$$

where $t_{proc\_data\_frame}$ is the MAC processing time of the data frame. In practice this figure is calculated putting the MT and the AP together and measuring the *RTT*, because in that situation the propagation delays of the frames are supposed to be zero, so that $t_{proc\_data\_frame} = RTT_0$.

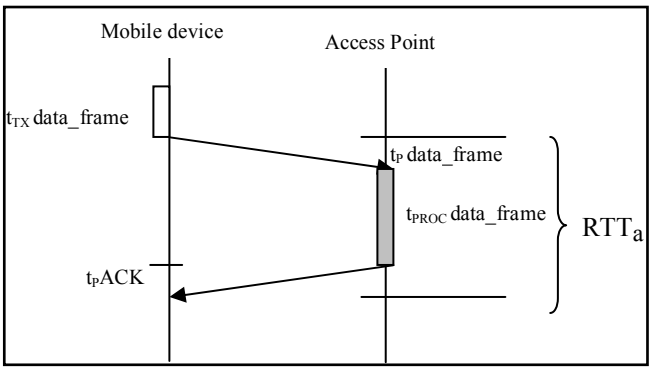

Figure 1. *RTT* measurement using IEEE 802.11 data/ACK frames

This $t_{proc\_data\_frame}$ figure is supposed to be constant over the time for a specific model of AP implementing a specific physical layer (e.g. the physical layer of IEEE 802.11b) because it corresponds to the short interframe space (SIFS) period, which is independent of the traffic load and other network and environmental parameters. This means that, theoretically, it is only needed to obtain this processing time (RTT_0) once, being valid from that moment for all the distance estimations.

B. The time measurement

As nowadays the IEEE 802.11 standard does not include high resolution timestamps in packet transmission and reception, a pure software solution to accurately measure *RTT* had to be discarded. As mentioned above, in [15] authors presented a technique to measure *RTT* between WLAN nodes without using additional hardware, but the achieved time resolution (1 μs) and then the ranging accuracy (errors around 8 meters) were not high enough according to our purposes. Furthermore, an additional special node was needed for the measurements. In our case it was decided to use the available clock at 44 MHz (f_{clk}) in the WLAN card of the MT to be located as the time counter, so that a timing resolution of 22 ns was achieved. Taking this fact and equations (1) and (2) into account, the formula for the distance estimation is as follows:

$$a = c \cdot \left(\frac{RTT_a - RTT_0}{2} \right) \cdot \left(\frac{1}{f_{CLK}} \right). \quad (3)$$

On the other hand, the triggers to start and stop the time counting - transmission of the last bit of the data frame and reception of the first bit of the ACK frame respectively- were also extracted from the chipsets of the MT's WLAN card. This approach entailed the design and implementation of a prototype, see [16] for more details.

C. Statistical processing

RTT is dealt with as a random variable, because *RTT* measurements carried out with the developed prototype presented noticeable time variability (see figure 2 with histograms of 1000 *RTT* measurements for distances of 0, 6, 12, 18, 24 and 30 m). Hence several *RTT* measurements are required for estimating a single *RTT* whatever the distance between MT and AP is. Afterwards, a proper statistical estimator (average, half range, mode…) is applied in order to mitigate as much as possible the noise.

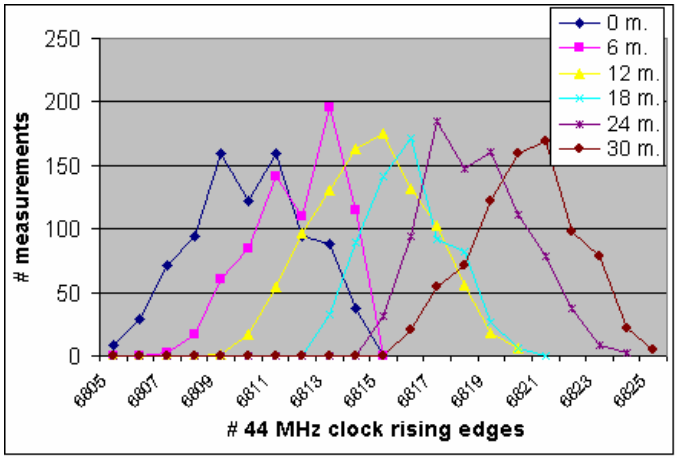

Figure 2. *RTT* histograms for 0, 6, 12, 18, 24 and 30 m.

Taking this into account, several statistical methods were evaluated in order to estimate *TOA* (see [16] for more details) with the *RTT* measurements carried out with the prototype for distances between 0 and 30m., in indoor environment and Line Of Sight (LOS) situation between the MT (in that case the prototype) and the AP. The method that provided the best accuracy turned out to be separately estimating RTT_a and RTT_0 using different estimators: $\eta - (\sigma/3)$ for the former and η for the latter (where η is the average and σ the standard deviation of the *RTT* measurements). This method exploited the fact that RTT_0 and RTT_a are of a completely different nature: RTT_0 is only MAC processing while RTT_a contains propagation time. The average is a good statistical estimator for the processing time, but relevance of lower measurements is higher for radio signal propagation time, suggesting the use of estimators smaller than the average. Hence the distance formula expression according to Eq. (3) finally was:

$$a = c \cdot \left(\frac{\left(\eta_a - \frac{\sigma_a}{3} \right) - \eta_0}{2} \right) \cdot \left(\frac{1}{f_{CLK}} \right) \qquad (4)$$

In practice η_0 is 6810.28 44MHz clock cycles. Table I shows the ranging results obtained using Eq.(4). The average of the resulting absolute distance-estimation errors, taking into account all tested distances, is 0.81 m.

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

Dist (m.)	RTT Standard deviation	RTT_a est. $\eta - (\sigma/3)$	Distance est. Eq (4)	Error (m.)	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

D. *Number of RTT measurements needed*

It is important to know the number of *RTT* measurements needed to estimate the RTT_a and RTT_0. This number is relevant in order to find a reasonable trade-off between bandwidth used, time employed and accuracy obtained. Since *RTT* is a random variable and an average-based parameter is used as estimator, the number of *RTT* samples can be set from a target confidence interval of the estimated average –around the population average- for a certain confidence level.

The formula of the confidence interval depends on the premises that can be assumed regarding the *RTT* distribution and a minimum number of samples needed that is accepted. In this case, since *RTT* distribution is not normal and 100 is accepted as the minimum number of samples, the formula is (for a confidence level of 95% of the time):

$$\eta \in (\overline{x} \pm z_{0.975} \cdot \sqrt{S^2 / n}), \qquad (5)$$

where η is the estimated *RTT* average, $\overline{x}$ is the population average, S the estimated standard deviation from the population and $z_{0.975}$ the z function value for a confidence level of 95%. The units for this confidence interval are 44 MHz clock cycles. From Eq. (5), n can be deduced:

$$n = (2 \cdot z_{0.975} \cdot S / A)^2, \qquad (6)$$

where A is the width of the confidence interval. The value of the z function for 0.975 is 1.96, the estimated standard deviation from the population (S) is 2. Taking into account that every 44 MHz rising clock implies a distance of 7 m., it was considered that only values of A under 0.5 (it is 0.25 rising clocks around the population average) had to be accepted. A result n = 246 was obtained; being aware that usually a small portion of the performed *RTT* measurements are not valid (due to errors of several types), n = 300 seemed to be a conservative figure to accurately estimate the *RTT*.

These 300 measurements are carried out in approximately 1.5 seconds with the ranging prototype described in [16], being the bandwidth used for distance estimation of 51.20 Kbps, less than 0.46 % of the total IEEE 802.11b bandwidth (11 Mbps).

III. RANGING PROBABILITY DISTRIBUTION

Finally, in order to obtain a statistical characterization of the system accuracy, the probability density function (PDF) of the distance estimation is calculated. The PDF is obtained normalizing an empirical histogram, which is calculated taking into account a large number (500) of distance estimations at a fixed distance (11 m.) –this is performing 500 series of *RTT* measurements- carried out using the ranging prototype with the described statistical processing. To this end, a *RTT* measurements campaign was carried out indoors at 11m. between the prototype (MT) and the AP., in LOS situation between them. Both the MT and the AP were placed

1.5 meters above the ground in order to preserve the Fresnel zone. According to Section II.D, the number of *RTT* measurements for a series is 300. As stated in Section II.A, an initial calibration at 0 distance is needed.

Ideally, all the distances measured should be 11 m; however, due to several error sources, the ranging system obtains distances from 8.80 m to 12.80 m. Comparing the resulting PDF with known probability distributions, it was found that the one that best fits it was a Gaussian distribution with η = 11.12 m. and σ = 0.84 m., as can be appreciated in Figure 3. This statistical model is also valid for other distances, because the distance estimation results presented in Section II.B and [16] show that there are no major differences in terms of error.

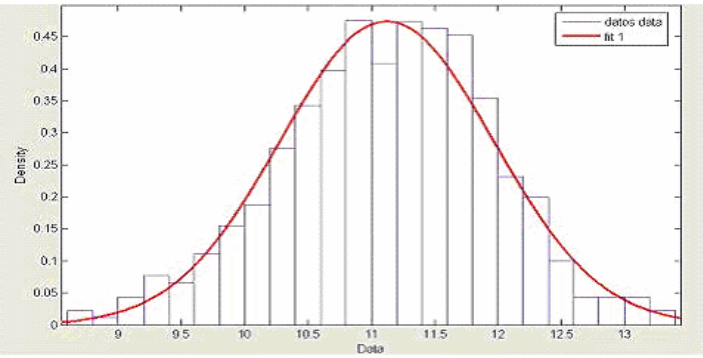

Figure 3. PDF of distance estimation

IV. Application to Positioning

A. Introduction

As explained in Section I, the main application of the described ranging method is the position estimation of the MT. In order to assess the basic positioning accuracy that the presented ranging technique is able to provide, trilateration simulations fed with actual distance estimations have been performed. Trilateration is the simplest way to obtain the MT position once the distance estimations from the MT to a set of AP are obtained and the AP's coordinates are known. It has to be underlined that the presented results constitute only a basic assessment of the positioning capabilities, further research should be performed in order to maximize the accuracy using for instance tracking capabilities instead of pure positioning or considering new trilateration approaches.

For 2D trilateration, at least three APs need to be involved. For details about the mathematics related with this topic see [17] and [18]. The trilateration algorithms that have been used are the Non-Linear Least Squares (Newton) and the Independent time GPS Least-Squares, both with the Linear Least-Squares algorithm for the initial raw position estimation that they need to start the process ([17],[18]). The distance estimation data used in the simulations are the ones obtained through real measurements with the developed prototype and correspond to the ranging statistical model presented in Section III.

B. Simulations

Several simulations –i.e. position estimations- were performed, each carried out as follows:

- The positions of the three APs and the true position of the MT (which was going to be estimated) were introduced.
- The simulation program calculated the exact distances from each AP to the MT. These distances were modified using the probability distribution of the distance estimated, this is the Gaussian distribution presented in Section III, obtained from true measurements performed with the implemented prototype. The same type of probability distribution was used for all distances because previous results show that there are no major statistical variations depending of the true distance (see Figure 4).
- A large number of MT's position estimations were performed with the trilateration algorithm, taking as inputs for each one a different combination of the distance estimations from the ranging probability distribution of the three APs. Thus all the position estimations were obtained considering all the possible combinations of the distance estimation figures taking into account the ranging model. Then they were subtracted from the MT's real position to find the position estimation errors.
- Finally, the cumulative probability function (CDF) of the position estimation error was found.

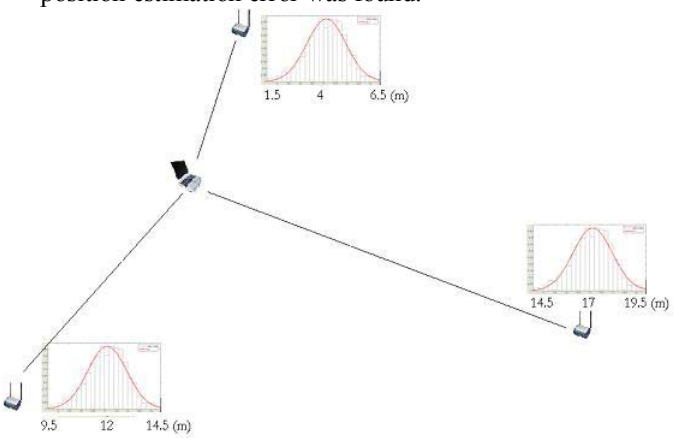

Figure 4. Trilateration with the distance estimation model

The simulations considered several scenarios because the results depend on the relative geographical situation between the MT and the three APs. Since APs are assumed to be rationally deployed (non-colinearly, for instance), the geometric dilution of precision (GDOP) [19] in representative scenarios is expected to be good. In a scenario in which the MT is located within the triangle formed by the three APs (i.e. best case), accuracy is superior to 1.4m. for the 66 % of the cases (see CDF of the positioning error in Figure 5). In a situation in which the MT is not within the triangle of APs but APs are properly deployed (i.e. GDOP is not bad, no alignment of APs). Accuracy is better than 1.8 m. with a probability of 66 % (Figure 6). It can be also seen that the Nonlinear Least Squares (Newton) algorithm outperforms the GPS Least Squares algorithm in both cases. The situation of some of the APs being in Non Line of Sight (NLOS) with

respect to the MT has not been considered in this contribution and it constitutes an important topic for further research.

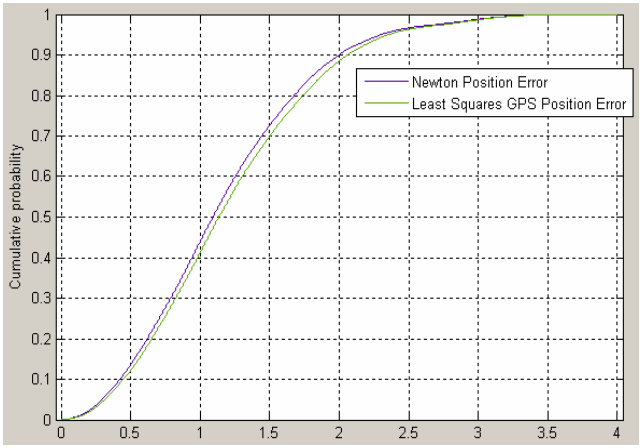

Figure 5. CDF of positioning error (I)

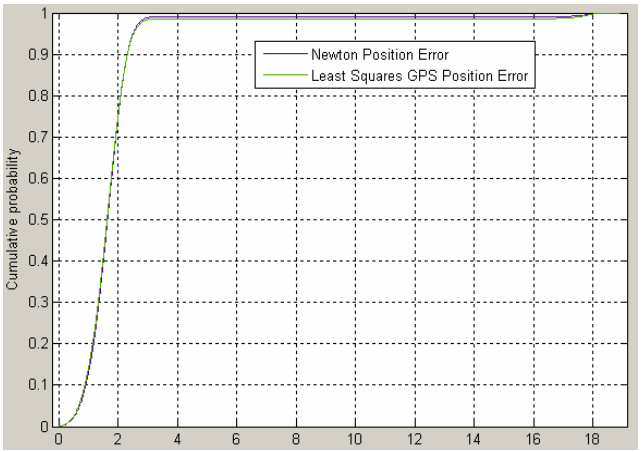

Figure 6. CDF of positioning error (II)

V. CONCLUSION

This contribution proposes a *TOA*-based technique for estimating distances between WLAN APs and terminals in IEEE 802.11 networks. The proposed approach is based on performing *RTT* measurements using standard data/control frames at the IEEE 802.11 MAC layer and a time counter module with the WLAN card clock. The approach presented for statistically processing *RTT* measurements (obtained with an implemented prototype) is described and evaluated. The selected statistical approach has the reduction of several noise sources as a goal and employs different estimators for both the *RTT* at the unknown distance and the *RTT* at zero distance. The results after this statistical filter show a ranging accuracy superior to 1 m. This confirms that accurate ranging can be achieved by means of a pure-software solution if the IEEE 802.11 packets are time-stamped using the available clock in the WLAN card. Finally, as an application, it has also been demonstrated that the results of this research can be directly used to feed an indoor location calculator through trilateration. This would allow to improve the performance level with regards to other existing WiFi-based location proposals mainly in terms of accuracy, flexibility and cost of deployment.

ACKNOWLEDGMENT

This research was funded by the EC under the Sixth FP IST LIAISON Integrated Project and by the Spanish Government and FEDER through the Plan Nacional de I+D (TIC 2003-01748 and TEC2006-09466/TCM).

REFERENCES

[1] N. B. Priyantha, A. Chakraborty, H. Balakrishnan, "The Cricket Location-Support system", *Proc. 6th ACM MOBICOM*, Boston, MA, August 2000.

[2] CSIRO's indoor position location technology project: http://www.csiro.au/csiro/content/standard/ps198,,.html

[3] Active Bats System (University of Cambridge) http://www.cl.cam.ac.uk/research/dtg/research/wiki/BatSystem

[4] Topaz: http://www.tadlys.com/pages/Product_content.asp?iGlobalId=2

[5] P. Bahl, V.N. Padmannabhan, "RADAR: An In-Building RF-based Location and Tracking System", *Proc. of the IEEE Conference on Computer Communications (INFOCOM '00)*, March 2000.

[6] P. Bahl, V.N. Padmanabhan, "Enhancements to the RADAR User Location and Tracking System", *Technical Report MSR-TR-2000-12, Microsoft Research*, February 2000.

[7] M. Youssef, "Horus: A WLAN-Based Indoor Location Determination System", *Department of Computer Science, University of Maryland*, 2004.

[8] P. Castro, P. Chiu, T. Kremenek, R. Muntz, "A probabilistic location service for wireless network environments", *Ubiquitous Computing 2001*, September 2001.

[9] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, X. Gao, "A wireless LAN based indoor positioning technology", *IBM J. RES. & DEV.* VOL. 48 NO. 5/6, September/November 2004

[10] A. M. Ladd, K. E. Bekris, G. Marceau, A. Rudys, D. S. Wallach, and L. E. Kavraki, "Using wireless Ethernet for localization," *in Proc. IEEE/RJS Int. Conf. Intelligent Robots and Systems*, vol. 1, pp. 402–408, Sept.-Oct. 2002

[11] Ekahau Positioning Engine: http://www.ekahau.com/

[12] M.Bocquet, C.Loyez and A.Benlarbi-Delai, "Using enhanced-TDOA measurement for indoor positioning", *IEEE Microwave and Wireless Components Letters*, 15(10), pp.612-614, 2005.

[13] 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.

[14] D. McCrady, L. Doyle, H. Forstrom, T. Dempsey, M. Martorana, "Mobile Ranging Using Low-accuracy Clocks", *IEEE Transactions on Microwave Theory and Techniques*, Volume 48, Issue 6, pp.951-958, June 2000.

[15] A.Günther, C. Hoene, "Measuring Round Trip Times to Determine the Distance Between WLAN Nodes", *Networking*, pp. 768-779, 2005.

[16] M.Ciurana, F.Barceló, F.Izquierdo, "A ranging system with IEEE 802.11 data frames", *IEEE Radio and Wireless Symposium 2007*

[17] W. Murphy, W. Hereman, "Determination of a Position in Three Dimensions Using Trilateration and Approximate Distances", *tech. report MCS-95-07, Colorado School of Mines*, Golden, CO, 1995

[18] G. Strang, "The Mathematics of GPS", *SIAM News*, Volume 30, Number 5, June 1997 © 1997, Society for Industrial and Applied Mathematics.

[19] N. Levanon, "Lowest GDOP in 2-D scenarios", *IEEE Proc. Radar, Sonar Navig.*, vol. 147, N.3, June 2000