Localization on IEEE 802.11 Networks

A. M. Vegni, *Student Member, IEEE*, and A. Di Nepi, *Member, IEEE*,

***Abstract*—In this paper we introduce an innovative technique for localization purpose in IEEE 802.11 networks, [1]. Our location algorithm is based on the distance estimation performed by three Base Stations (BSs), employing the triangulation process to calculate the mobile user position. This method results innovative and efficient both for the IEEE802.11 PCF and DCF phases to track the user position at a constant rate according to the user speed. A complete simulation model has been developed to assess the maximum number of users traceable.**

Then, in the last part of the paper, we investigated the use of an algorithm for the time of arrival (ToA) estimation based on the OFDM modulation, employed in IEEE 802.11a and 802.11g. We estimated the attenuation and the phase rotation at the receiver side, for each sub-carrier, [2]. Using a Kalman filter, we also evaluated the time of arrival and the distance between two mobile nodes.

***Index Terms*—Network localization, wireless networks, Kalman filter.**

I. INTRODUCTION

WIRELESS communications are an increasing reality, developing to the nomadic environment. The mobility management is the essential support for roaming users with mobile terminals to permit them to enjoy their services when they move from a cell to another.

Integration of localization services in wireless networks is an open issue. The focus is to verify if existing wireless networks can support localization services, specially for environments where satellite communications are not present. In this way, no modification on layer protocols and on throughput parameter can occur. This condition is acted on the basis of instantaneous bandwidths that are compatible with required accuracy.

The location techniques are then the basis of a new class of services: the so called "Location Based Services" (LBS) that have to provide to the user the appropriate contents, to the right place and in the most simple and rapid way.

The new scenario includes a wide range of services based on the possibility to track and navigate the user in a location-aided environment. Such innovative services include: emergency and rescue assistance, security, protection and control, user location and navigation, and so on. Some of the actual location systems are widely used in the outdoor environment (GPS/GALIELO) while they are still barely used in the indoor.

Our aim is to complement WLAN networks with location services for indoor environment. Indoor location is solved for a single user position estimation, [6] and [7], while multi user tracking at the MAC level is an open issue. We investigate the actual IEEE 802.11 limits in terms of number of maximum tracking users.

In Section II the proposed localization algorithm is described. Sections III and IV present, respectively, an assessment of the maximum number of traceable terminals and the simulation model.

Then, in Section IV we propose an innovative algorithm for the Time of Arrival (ToA) estimation based on the OFDM modulation. A "real" test case was implemented to prove the effectiveness of the proposed algorithm, (Subsection B).

ToA estimation depends on the instantaneous bandwidth, that is able to assure a good accuracy for typical real SNR values. So, we focused on localization services integration on wireless networks, maintaining the same wireless protocol characteristics.

A. M. Vegni, and A. Di Nepi are with the Department of Applied Electronics, University Roma Tre, Rome I-00146, Italy, e-mail: (amvegni, dinepi)@uniroma3.it

II. LOCALIZATION ALGORITHM IN IEEE 802.11 NETWORKS

The location technique is based on the triangulation method [6]. Basically, at the PHY level any distance estimation algorithm can be used [9]. The position estimation for several MT can be performed considering two different phases, the IEEE 802.11 PCF (Point Coordination Function) and DCF (Distributed Coordination Function) [3], [4], and [5]. In the first case, AP acts as Point Coordinator (PC), while in the second one coordination is directly adopted by the different stations.

In our proposed method, we use PCF to periodically query the MT at a rate that depends on their mobility class, while in DCF mode we collect all the distance estimation performed by the BS. Exploiting the PCF mechanism the system is able to provide near isochronous polling request to the MT avoiding the collisions typical of the DCF phase ensuring also Quality of Service for a certain number of users.

During the association phase with the AP, the MT requires to be inserted in the Location List, declaring its mobility class. We considered three different mobility classes:

- no mobility: fixed station, the position is calculated during association;
- low mobility: low speed user, e.g. a man walking;
- high mobility: high speed user, e.g. small luggage machinery moving in an airport passenger area.

Defining different mobility class allows optimizing the bandwidth usage based on the user needs. High speed corresponds to high location update rate.

The Location List includes a list of MTs and the correspond update rate pair. It is similar to the PCF Polling List, where the subscribed MTs are periodically queried by the AP during the PCF phase to broadcast a Location Packet which is then use by the BS to estimate their distance from it.

The location algorithm has the following steps:

1. Location Update Request: right after the BEACON packet at the beginning of the super-frame the AP, that is the Point Coordinator, queries the first MT of the Location List which needs a position update to broadcast a Location Packet. The Location Update Request packet is sent from the AP/PC to the MT directly addressing the latter with its address.
2. Location Packet Broadcasting: the MT responds to the Point Coordinator request broadcasting a Location Packet during the CF-UP phase of the PCF (after a SIFS period

has been elapsed). Such Location Packet is received from the entire BS set that "see" the MT.

3. MT-BS Distance Estimation: each BS that has successfully received the MT Location Packet estimates, with a PHY method (i.e. estimating TOA) its distance from the MT.
4. Collect: the BSs transmit back their distance estimation set to the AP during the DCF phase. If the BS has computed several estimations for different MT, in order to save bandwidth usage, it sends only one data packet including all the estimations.
5. Position Computation: finally the AP, once received all the BS estimations, computes the MT position. At least three distance estimation are needed to calculate the user position. On the following Location Update Request, the AP sends back to the MT its position at the previous instant.

The overall process is repeated at the multiple of Location Update Rate, typically chosen as a multiple of the super-frame duration. Of course, more than one user could be localized during the same super-frame; in case of busy network different user are distributed on different super-frame. In case there is any problem in the overall process (i.e. the MT does not respond during the CF-UP, the AP receive less than three different estimation) the position estimation is postponed to the following scheduled instant. The duration of the PCF phase is related to the number of MT included in the Location List and hence could be reduced by the AP/PC with a CF-END packet, in case it have completed to query the entire MT set.

III. Maximum Number of User Estimation

An estimation of the maximum number of user is evaluated in terms of localized MTs. The time frame necessary to poll a user and to receive back the broadcast packet on which the BS calculates the user position is limited by:

$$T = 2\frac{r_{max}}{c} + 2T_{SIFS} + \frac{D_{LUR} + D_{ACK}}{M} \quad (1)$$

where r_{max} is the maximum coverage area [m], c is the speed of light [m/s], T_{SIFS} is the SIFS interval duration, D_{LUR} is Location Update Request packet dimension [bit], D_{ACK} is Acknowledge packet dimension [bit], and M is the Data Rate [Mbps].

So, the number of users that the system is able to manage within one super-frame $(PCF + DCF)$ is given by:

$$N_{TOT} = \frac{\Delta T_{PCF_{\max}} - T_{SIFS} + \frac{D_{BEACON}+D_{CFEND}}{M}}{T + \varepsilon\left(\frac{r_{\max}}{c} + \frac{D_{LUR}}{M} + T_{PIFS}\right)} \quad (2)$$

where $\Delta T_{PCF_{\max}}$ is the maximum duration of the PCF [ms], D_{BEACON} is the BEACON packet dimension [bit], D_{CFEND} is the CF-END packet dimension [bit], T_{PIFS} is the PIFS interval duration, and ε is the performance reduction factor due to the coverage area and channel noise.

Combining the two expressions above, the maximum number of users the network is able to manage is:

$$N_{TOT} = \frac{\Delta T_{POLL}/\Delta T_{SUPERFRAME}}{\Im(N)} \quad (3)$$

where ΔT_{POLL} is the polling period of the same MT, $\Delta T_{SUPERFRAME}$ is the super-frame duration and $\Im(N)$ is the integer part of N.

As expected, the maximum number of users is strictly related to the Location Update Request time and hence to the mobility class of the users. In the simulation model we realized a localization system with 4 BSs and a square area: the BS was positioned at square vertex. Different network scenarios were considered, in order to highlight the best BS number and configuration as a function of stations coverage area and data rate.

In the simulated network environment, the main entity is the AP that allows the devices communication, manage the PCF phase and keep track of all the terminals that have to be track with the corresponding mobility class. Then, a certain number of BS is dedicated to the distance estimation, while a certain number of MT needs to be tracked.

The operating frequency is 2.4 GHz as stated according to the IEEE 802.11g standard. The distance estimation at the PHY level is performed with an algorithm that estimates the time of arrival of the BS received signal directly in the frequency domain exploiting the OFDM modulation [9].

Another critical parameter that directly affects the results is the data rate. So, we showed results for different data rate, ranging from 6 Mbps to 48 Mbps.

On the other hand, the maximum value of coverage area was limited to the inter-distance between the different BSs in order to reduce the collision due to the lack of visibility, called as the hidden terminal problem.

The coverage area was set equal to the maximum distance between the BS and the AP. The dimension of data packet used to poll the mobile terminals was fixed to 400 bit (272 MAC header bit and 128 for the data payload) and the ACK packet dimension to 112 bit, according to IEEE 802.11 standard. Along with data rate and packet length, we considered the time parameter necessary to transmit a single packet. It was expressed as:

$$T_{packet} = T_{computation} + T_{transmit} \quad (4)$$

Assuming that the computation time is negligible with respect of the other parameter, it results as:

$$T_{packet} = T_{transmit} = \frac{L_{packet}}{M} = \frac{400bit}{12Mbps} = 0.033ms \quad (5)$$

The time necessary to transmit a packet is direct function of the data rate. Assuming low speed users (in the range of 1-2 m/s), a good compromise for the Location Update Request rate is 500ms. Finally, typical times of an IEEE802.11 network chosen in our simulation were: SIFS = $28\mu s$, PIFS = $48\mu s$, DIFS = $68\mu s$, Minimum Contention Window period = $16\mu s$, Maximum Contention Window period = $4080\mu s$, Super-frame duration = $5ms$.

A. Simulation results

For a multiple mobile terminal scenario, we considered 6 BSs located on the hexagon vertex and one AP in the hexagon center. Figure 1 represents this configuration.

We putted the MTs random speed to 2m/s and the Location Update Request period to 0.5s. The data rate range spans from

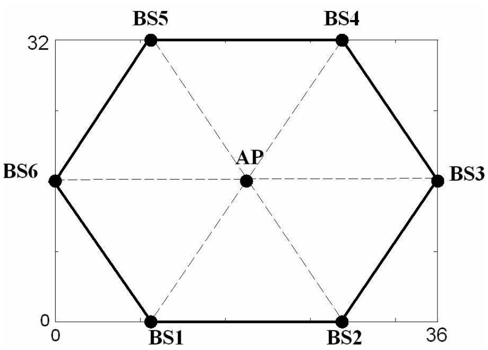

Fig. 1. 7 BS grid configuration, $36m \times 32m$.

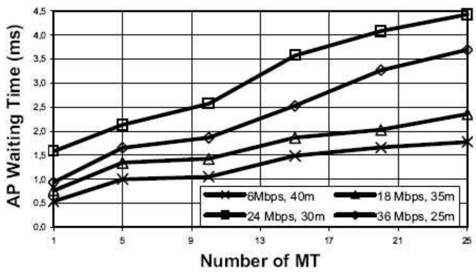

Fig. 2. AP Waiting Time for the multiple MT case.

6 Mbps to 26 Mbps, while the BS coverage area was fixed to the maximum value specified by the IEEE 802.11 standard for the specific data rate in indoor environment. For each case a number of different paths have been tried, each time varying the MT position, in order to consider the statistics of at least 1000 different points of the grid.

The output results were evaluated in terms of:

- AP waiting time. It is the overall time necessary to perform a position estimation, from the moment the AP query the MT to the time it receive back the BS estimations.
- Number of available BSs: it is the average number of BSs in the MT covered area. It is the number of BSs to the position estimation. This parameter depends on the coverage area, independently of the data rate selected.
- Number of used BSs: it is the number of BSs actually used, among the available ones.
- Location Probability: it expresses the probability that the AP has at least three distance estimation on which perform the triangulation.

Figures 2, 3 and 4 respectively represent the AP Waiting Time, the number of BSs used and the Location Probability as function of the number of MTs for four different data rate/coverage area values.

Figure 2 shows the increase of AP parameter as long as the number of MTs increases. This is related to the number of collisions increase due to the fact that the network traffic is increased. In the worst case, considering a delay of 4.5ms, from the Location Update Request moment to the reception of the position estimation, the terminal has been shift of few cm introducing an error less than 1% (each Location Update Request the MT has been shifted of 1m).

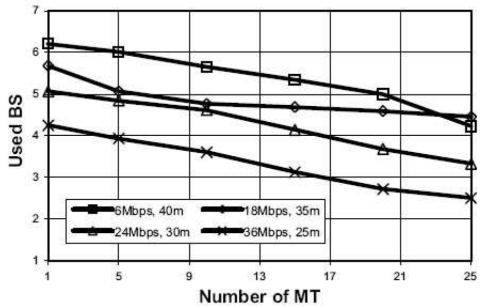

Fig. 3. Number of used BS for the multiple MT case.

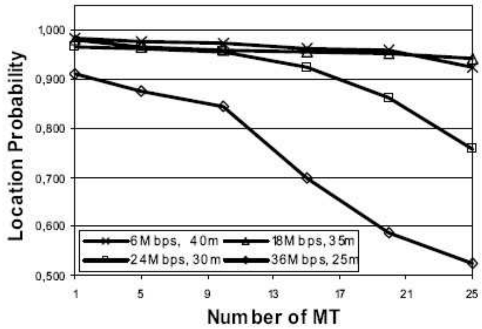

Fig. 4. Location Probability for the multiple MT case.

The number of used BS decreases with the number of MTs increasing, since the BSs have to send longer packet (containing more distance estimations) during the DCF phase, causing an increase in the number of collisions.

Finally, regarding the Location Probability, we note that to achieve better performance it is more important to have a high coverage area rather than a high data rate.

Simulations results are shown in Table A. With an average Location Probability of 80%, the AP receives at least three distance estimation of the 25 MTs for a BS coverage area greater than 25m, while the number of traceable MT drop to 17 for BS coverage area less than 25m.

Number of users	BS coverage area	Data rate
40	35m	18Mbps
23	30m	24Mbps
12	25m	26Mbps
3	20m	48Mbps

IV. ToA ESTIMATION ALGORITHM

To provide a localization service for a mobile terminal, a BS knows its location and its internal time reference is synchronised with the system timing. At least three base stations have be view by each MS to provide a localization service. To recover a time misalignments between them, more than three BSs are used. The BS could also be wired to provide a better time synchronization between them.

The architecture of the localization protocol was structured on the basis of network requirements, such as the estimation uncertainly, mobile terminal velocity, data rate and channel occupation.

The proposed algorithm provides ToA estimation by measuring the received signal phase. The whole algorithm directly applies to the OFDM modulation scheme.

As IEEE 802.11a and 802.11g divide the bandwidth in 52 sub-carriers, 48 of each reserved to data and 4 to control data (pilot), each OFDM receiver can provide 52 estimations of the received signal phase. The ToA and the distance could be estimated by the phase shift produced by the time delay. The estimation is done iteratively through a Kalman filter as described below.

For each batch of measures, at the output of receiver S values are available, where S is the number of sub-carrier ($S = 52$). Let $\Delta\varphi_m(h)$ of the m-th sub-carrier f_m is

$$\Delta\varphi_m(h) = -2\pi\Delta t(h) f_m. \tag{6}$$

We modeled the time delay variations induced by the user mobility with the first order, discrete time, dynamical system, driven by the white Gaussian noise, as

$$\Delta t(h+1) = \Delta t(h) + n(h). \tag{7}$$

We can rearrange the dynamical equations 6 and 7, by introducing a parallel to serial conversion of the phase shift sub-carrier array. So, we obtain

$$z(hS + m) = \Delta\varphi_m(h), \tag{8}$$

or equivalently

$$z(k) = -2\pi\Delta t\big[k - (k \bmod S)\big] f_{k \bmod S}, \tag{9}$$

with

$$h = k \bmod S \tag{10}$$
$$m = k - hS. \tag{11}$$

In addiction, we pose

$$a(hS + m) = \Delta t(h) \tag{12}$$

and we write the time delay dynamical equation 7 as

$$a(k+1) = \begin{cases} a(k) + n(k), & k \bmod S = 0 \\ a(k), & \text{otherwise.} \end{cases} \tag{13}$$

Finally, we can rearrange the dynamical equations as follows

$$a(k+1) = a(k) + w(k) \tag{14}$$
$$z(k) = -2\pi f_{k \bmod S}\, a(k) + v(k) \tag{15}$$

where $v(k)$ is a stichastic process that models the OFDM receiver noise and $w(k)$ is a white, zero mean, Gaussian stochastic process which model the estimation uncertainly due to fact the user has moved from the time of the previous OFDM packet, whose covariance is

$$R_w(k) = \begin{cases} \sigma_w^2, & k \bmod S = 0 \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

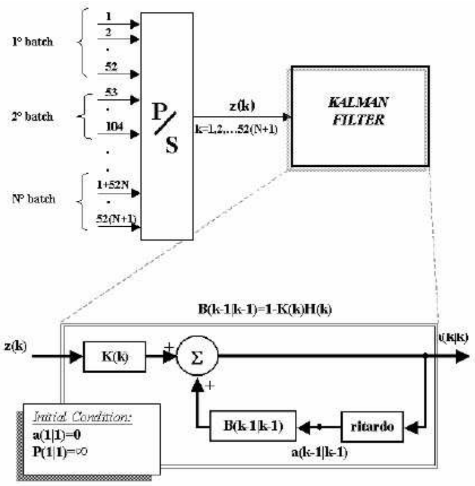

Fig. 5. Proposed algorithm for the ToA estimation.

We see that σ_w^2 is a function of the user mobility within two consecutive measurements. It depends on the user maximum speed v_{Max}, the maximum acceleration α_{Max} and the time interval between two measurements $\Delta\tau$, and it can be set as:

$$\sigma_w = \frac{1}{c}\Big[v_{Max}\Delta\tau + \frac{\alpha_{Max}}{2}\Delta\tau^2\Big]. \tag{17}$$

where c is the speed of the electromagnetic wave.

Regarding $v(k)$ process, we modeled it as a white, zero mean, Gaussian process with covariance matrix

$$R_v(k) = \frac{\sigma_N^2}{|b_{k \bmod S}|^2}. \tag{18}$$

Finally, the ToA estimate is extracted from the Kalman Filter only at the end of each batch, as Figure 5 shows.

$$\Delta t_{est}(h) = \hat{a}(Sh - 1/Sh - 1) \tag{19}$$

V. Simulation results for ToA estimation algorithm

A. Reference scenario

As first step in the performance assessment, we simulated a localization system with 4 BSs and a square area. Again, the BSs were positioned at square vertex and the MT randomly moves within such area. Due to the low user mobility, the changing in the update period results in a low increase of σ_w that is recovered by the Kalman filter.

We evaluated the distribution of the uncertainly on the ToA estimation and on the final position estimation after the triangularization, as Figure 6 and Figure 7 represent, respectively.

Then, we increased the number of BSs in the network and Figure 8 shows an effectiveness increase of the performance, for a typical case of $SNR = 30$dB. The first graph represents the uncertainly on the MS position, while the second one the uncertainly on the ToA estimation.

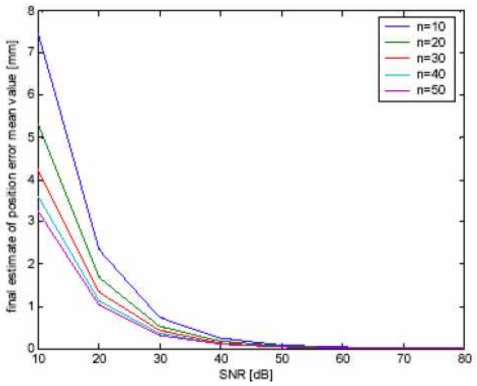

Fig. 6. Distance uncertainly vs SNR for different values of S.

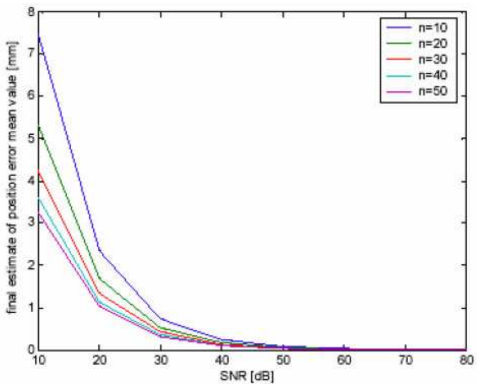

Fig. 7. Mean of the uncertainly on the ToA estimation varying the SNR and the number of iteration

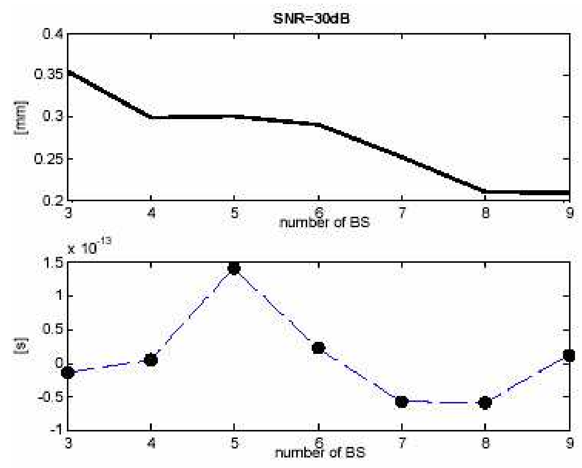

Fig. 8. Uncertainly on position and time estimation vs number of BSs

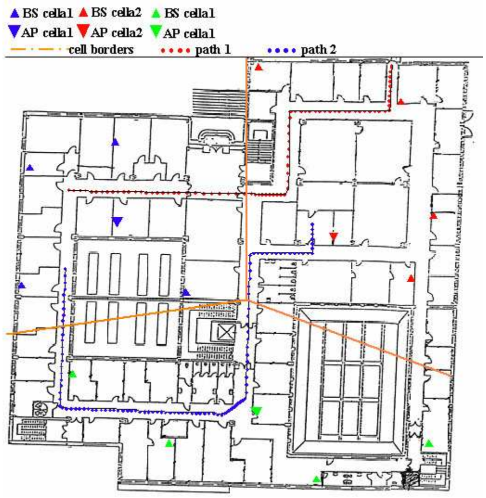

Fig. 9. Real test case simulation.

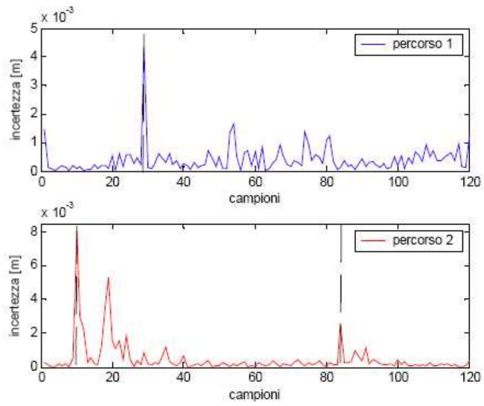

Fig. 10. Position estimation uncertainly vs time.

B. Real Scenario

For a more realistic evaluation of the performance, we then simulated the use of the localization system in the Applied Electronics Department of University of "Roma TRE", whose map is shown in Figure 9. We divided the whole area in three zones, where an AP and several BSs manage each one. This simulation is a "real" test case, proving the effectiveness of the proposed algorithm.

Each BS could measures only the MS in their zone. We supposed that the mobile user moves along the path indicated in Figure 9 with a variable speed for 60s. The dot lines represent the estimated position at the update time, while the continuous lines represent the real user trajectory. For each path 300 simulations has been done observing an uncertainly on the estimated position of 0.27mm and 0.65mm for the path1 and path2, respectively.

In Figure 10 we show the position estimation uncertainly along the path, where the peak represents the transition between different zones. The performance within the different zones depends on different BSs positioning with the respect to the MS.

VI. Conclusion

In the first part of this paper, an innovative technique for localization purpose in IEEE 802.11 networks was investigated. The proposed algorithm exploits the IEEE 802.11g super-frame structure including both the PCF and the DCF phases. The analysis shows that with low mobility network users the algorithm is able to locate all the users. The algorithm implementation with the actual IEEE 802.11 devices present best performances for outdoor or open indoor environments, (i.e. airports, train stations, museums, etc.).

Then, a localization service algorithm for IEEE 802.11 networks was proposed, based on the OFDM modulation scheme. It iteratively estimates the received signal phase using a Kalman filtering technique. The performances are better than the traditional ones using the RSSI technique. Finally, a real test case with different cells was presented.

Future works are addressed to implement the localization algorithm in WiMax Mesh scenarios.

References

[1] A. Di Nepi, G. Massaro, M. Carli and A. Neri *MAC Location Services for IEEE 802.11 Networks*, Proc. IEEE 5th International Conference on Networking, ICN'06, April 23-28, 2006 Mauritius,

[2] D. Giorgi, A. Di Nepi and A. Neri, *OFDM Localization Technique*, ICN 2004 February 29 - March 4, 2004 Gosier, Guadeloupe, French Caribbean.

[3] IEEE 802.11 Standard, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 1999.

[4] Standard IEEE 802.11a, *Supplement to IEEE Standard for Information technology: High-speed Physical Layer in the 5 GHz Band*, 1999.

[5] Savarese, Jan M. Rabaey, Jan Beutel, *Location in distributed ad-hoc wireless sensor networks*, Proceedings of the IEEE, vol.4, pp2037-2040, Maggio 2001.

[6] Neal Patwari, Robert J. ODea, Yanwei Wang, *Relative Location in Wireless Networks*, Vehicular Technology Conference of the IEEE, vol.2, pp1149-1153, Maggio 2001.

[7] Paramvir Bahl and Venkata N. Padmanabhan, *Enhancements to the RADAR User Location and Tracking System*, Proceedings of the IEEE, Febbraio 2002.

[8] Homayoun Hashemi, *The Indoor Radio Propagation Channel*, Proceedings of the IEEE, vol.81, pp943-968, Luglio 1993.

[9] Mohinder S. Grewall, Angus P. Andrews, *Kalman filtering: theory and practice using MATLAB*, Wiley-Interscience Publication, 2001.