NetArgus: An SNMP Monitor & Wi-Fi Positioning, 3-tier Application Suite *

George E. Violettas, Tryfon L. Theodorou, Christos K. Georgiadis
University of Macedonia, Thessaloniki, Hellas
Email: {georgevio, mai0730, geor}@uom.gr

Abstract— **The paper describes the necessary fields investigated for creating an application that is able to monitor any kind of network, wired or wireless, with all its possible aspects. In the same application, we also implemented original algorithms for finding the position of a moving station, utilizing the signal level of the wireless protocols 802.11 devices (Wi-Fi). Field research and exhausting sampling was done, in order to resolve the various practical problems faced, according to the signal level of the wireless stations and the hardware involved (cables, antennas etc). Also various flows and looseness's were discovered of the 802.11 protocol, like the lack of definition of the signal level and its range width. Various practical problems of the positioning issue have been satisfactory managed. A 3-tier application was created, capable to draw paths and manipulate proper information from various network moving clients, using low level operating system libraries and SNMP.**

Keywords- FSPL; dB; dBm; monitoring wireless networks; RTLS; SNMP; SNR; Wi-Fi positioning;

I. INTRODUCTION

The aim of this essay was to use the Wi-Fi available information for finding the position of a station equipped with it. In addition, SNMP protocol was used for a central management of such devices.

Practical problems of positioning were solved, by creating the "NetArgus" application, which draws information from network devices using various low level operating system libraries like Microsoft WMI and NDIS.

The application implemented is open, it permits any kind of parameterization and it fully exploits all the new technologies. It is modular; it consists of 3 basic segments, providing the ability to install every part of it to the most convenient part of the network. The GUI user part is location independent.

The above mentioned application was created in order to manipulate all the necessary information. An SQL database stores in real time the SNMP available information together with the signal level information sent by the moving stations through the application created for that purpose. A server application derives data from the database and it calculates in real time the position of the moving stations. The client application is picturing in a 2-axis graphical interface the position of the network elements.

The theoretical barrier of the 802.11 signal level strength measurement is analyzed, due to limitations to the implementation of the specific variable (integer number in a logarithmic function).

II. RELATED WORK

All the systems finding the location of a moving target (positioning) are called RTLS (Real Time Location System).

"Cisco" has implemented such a system addressed mainly to closed spaces. It combines software and hardware (wi-fi tags), it is a closed commercial system, cooperating with various vendors hardware [1]. "Aeroscout" is the first company introduced on 2003 an RFID tag compatible with Wi-Fi, so it is possible to find the position of the target carrying this tag [2].

The closest to our implementation is the "Ekahau" system, a closed commercial system. It operates in open and close spaces and it seems to dominate the market, basically because of the accuracy provided, but also because it is not using any hardware, being able to cooperate with various systems and vendors [3].

Most of the papers investigated were vague (probably on purpose, due to the future commercial applications).

A demanding job is described in [4]. It describes the possibility of physically locating the position of a wireless intruder into a corporate network. An interesting job is described in [5]. They faced the same problems, like extracting the signal level info (without revealing much), the statistical error, and the distance from the broadcasting station. In [6] the extraction of the signal level through SNMP is described. We shall see that this is not always possible. The essay in [7] has some very interesting ideas, and it was the main inspiration for the "Kalman" filter future work.

So far we are not aware of a work combining SNMP with Wi-Fi positioning.

III. PAPER STRUCTURE

In section IV there is a small introduction to SNMP and Wi-Fi Networks. In section V.A there is a detailed description of the signal level (RSSI) of a Wi-Fi moving client and its weakness. In VI the theoretical background of finding the position through triangulation is described. Chapter VI.A describes the equation of the signal level compared with the distance (FSPL). Sections VI.C & VI.D describe the practical distance limits of the signal level and the difference of representation of the SNR versus RSSI (dB versus dBm).

In section VII the implemented system (NetArgus) is described along with its main features and advantages.

** Paper Presented at IARIA - ICWMC 2009, at Cannes/La Bocca, France, winning the "Best Paper Award" price*

At last, there is a section (IX) with feature work, and some possible alteration and expansions of the system.

IV. BACKGROUND

A. SNMP

SNMP (Single Network Management Protocol) is a set of simple set of instructions or applications and the data that those instructions are collecting. Given this information and the possibility of sending commands for altering state, the administrators of a network can *"…control the speed and the workload on a specific interface of a router, or continuously monitor the working temperature of a switch and interact with it according its levels…"* [8].

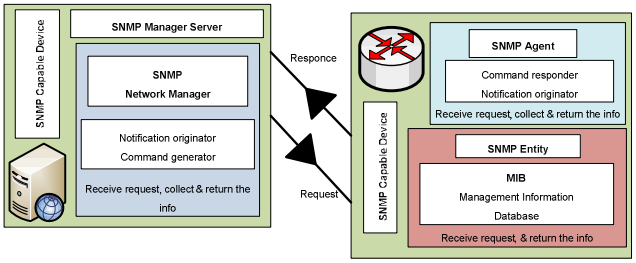

Figure 1: SNMP, How it works

A simple SNMP System is depicted in Figure 1.Compatible devices are devices such as computers, routers, switches/hubs, terminal servers, cameras, etc. [9].

B. Wi-Fi (802.11x) Networks

Wi-Fi networks do not need an installation permit all over Europe, operating at the frequency of 2,4 GHz.

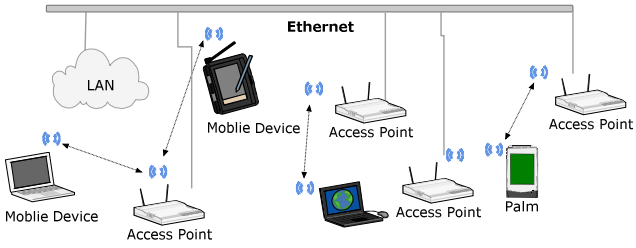

Figure 2: Typical Wireless Network & Roaming Clients

In a typical installation of such a network, an efficient number of Wi-Fi Stations (Access Points, APs) strategically placed, are covering a given area with wireless signal. Within this area, as it is depicted in Fig. 2, certain wireless capable devices are moving around, such as laptops, wireless enabled devices, smart phones, PDA's etc.

V. WI-FI SIGNAL STRENGTH

In such networks, every moment, each client is connected to a particular AP. When the moving client is not receiving any more an adequate level of signal, then it has to connect to another AP (if available). In order to decide that, it has to know which station is closer to it, obviously by comparing the signal level. In theory this signal level, is monitored from both parties (AP & moving client) [12][13]. In practice, there are several devices that are not monitoring at all this information. As a result, information from the moving client is needed. The moving client is continuously monitoring the signal level from the AP it is connected to, plus the signal level of all the APs within its reach.

As soon as the Wi-Fi client knows the signal level from at least 3 nearby stations, its position can be triangulated.

A. RSSI

IEEE 802.11 describes "…*RSSI is an optional dimension, varying from zero to max, its accuracy is not described, and it has a meaning only as a relative number (SNR)* …" [14]. The size of this information is defined at page 600, as having 0-255 different levels, (one Byte). According to Microsoft [15], RSSI is an optional field, implemented as a signed integer. In all the occasions we managed to investigate, RSSI was a signed (usually negative) integer. Depending on the manufacturer, it usually takes values from -20 to -95 dBm.

One of the primary "position finder" error factors is the RSSI nature. Because it is an integer, it necessarily alters its values very easily. Empirical studies showed that even when the moving station is in immobility, the RSSI value usually continuously jumps from one integer to the next. The following table shows that the least error on the RSSI, can bring an error of at least 2 meters.

TABLE I. RSSI VS DISTANCE*

fspl (dBm)	*Distance (m)*
65	17,38
66	19,5
73	43,65
74	48,98
83	138,06

* Those prices come from the function fspl=20log$_{10}$d+2log$_{10}$f+32,44, if we replace *f*=2440000 Hz, and fspl with the table's values. If we substitute two following values to the fspl (for example 65 & 66 dBm) we see that the difference is approximately 1,2 meters. Due to the logarithmic nature of the mentioned function, the error increases as the fspl prices increase.

Several low level Microsoft libraries are needed for extracting the RSSI information of a Wi-Fi client equipped with Microsoft Windows XP Operating System. WMI library [16] and Native Wi-Fi library [17] can not be used, due to bugs according to [18] [19] or lack of uniqueness in the association of that information with the SSID (Service Set IDentifier, the -user set- name of the network). The only useful library, proved to be NDIS [20]. The combination of the AP's Mac Address with the RSSI information made it possible to construct a useful unique set of information. The particular combination proved to be manufacturer independent.

VI. POSITION FINDING USING SIGNAL LEVEL

Given a well known area (x,y), in order to find the relative position of a moving station within this area, the station's distances from at least 3 well known spots (APs)

* *Paper Presented at IARIA - ICWMC 2009, at Cannes/La Bocca, France, winning the "Best Paper Award" price*

are needed. Those distances can be calculated using the signal level between this moving station and the APs (Fig. 3).

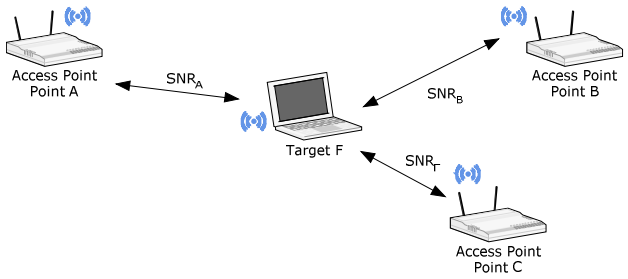

Figure 3: Triangulation of a moving station

The three equations describing the signal level are:

$$SNR_i = f(di), i \in \{A, B, C\} \quad (1)$$

Solving them for the unknowns X_F, Y_F, yield the following three equations for two unknowns:

$$dA = g(X_F, Y_F) \quad (4)$$

$$dB = j(X_F, Y_F) \quad (5)$$

$$dC = h(X_F, Y_F) \quad (6)$$

Those two unknowns are the co-ordinates of the moving station $F(X_F, Y_F)$.

A. Signal to Noise Ratio - SNR

SNR is the logical product of the signal level (S) to the noise level (N in Watts, so the result is just a number [21].

$$SNR = 10\log_{10}\frac{S}{N} \quad (7)$$

The logarithm of this product is used, which has different levels to the different ends of a system. We usually use it at the end of the antenna, unless differently stated [22]. SNR is always calculated in dB (decibels).

B. Free Space Path Loss (FSPL)

FSPL as is depicted in Fig. 4, is the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space, with no obstacles nearby to cause reflection or diffraction [23] [24].

$$fspl(dB) = 4\pi d\lambda^2 = 10\log_{10} 4\pi dfc^2 = \\ = 20\log_{10} d + 20\log_{10} f - 147,56 \quad (8)$$

where:

- $\pi = 3,14\ldots$
- d = distance (in meters)
- λ = wavelength (in meters)
- f = frequency (in Hertz)
- c = Speed of light = 2,99792458 * 108 m/sec

In the literature frequency (f) is often found as equal to 2.400GHz. That is inaccurate because frequency takes prices from 2400GHz to 2483GHz depending on the country implemented.

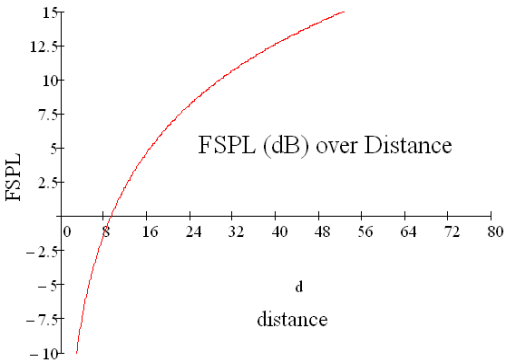

Figure 4: FSPL over distance

If the signal level is known, (8) becomes:

$$d = 10^{\left(fspl - 20\log_{10} f + 147,56\right)/20} \quad (9)$$

C. Signal Level Usage Limits

According to practical observations, the above mentioned equation is useful only at the middle space of the distance involved. If the equation is to be used outside of some barriers, it inserts a big inaccuracy to the position finding process. Those practical barriers are known from the specifications of the 802.11 protocol [25] in conjunction with the FSPL equation. They can be roughly set between 10-80 meters. Because of the significant addition of antennas, cables and paraphernalia [26], it is better if we re-calculate those distances, taking in consideration the signal power (dB) generated after those additions. Practically we discovered that the limits of the signal power, are between -40dB and -90dB. Besides the fact that it is better not to use all the signal level information avaliable, for the shake of calculation speed, it is also because an extra information after a certain point, does not add any extra accuracy to the calculations [27].

D. SNR & RSSI (dB vs dBm)

SNR (7) is usually described as the ratio of a signal power to the noise power corrupting the signal [28]. Generally, dB's as measurement unit for the received power was used ad-hoc, and the documentation came later on [29]. The absolute power of a signal is declared by the same equation based on the previously known level of one milliWatt (1mW) [30]. So, (**7**) becomes

$$fspl(dB) = 20\log_{10} d + 20\log_{10} f - 147,56 \quad (10)$$

where P_1 is the received signal level, and P_2 is the transmitting power, P_2=1mW. The result is in dBm,

$$SNR(dBm) = 10\log_{10}\frac{P_1}{1mW} \quad (11)$$

** Paper Presented at IARIA - ICWMC 2009, at Cannes/La Bocca, France, winning the "Best Paper Award" price*

All the Wi-Fi cards on the market are giving the results of the signaling power in dBm's, e.g.

$$RSSI(dBm) = 10\log_{10}\frac{S}{P} \qquad (12)$$

where P is the 1mW base [26].

Converting RSSI to SNR is possible considering the signaling power of an AP as equal to 20 mW as stated at the protocols specifications. If the received signal power level is P, then (7) becomes:

$$SNR\left(dB\right) = 10\log_{10}\frac{P}{20mW} \qquad (13)$$

According to [24] we can add to the calculations, all the network elements as follows:

$$Rx = T_xPower - T_xCableLoss + T_xAntennaGain - fspl + R_xAntennaGain - R_xCableLoss \qquad (14)$$

- $Rx = Received\ Power$
- $T_x = Transmitted\ Power$

Because some of those variables cannot be accurately measured, it is a good idea to insert an S variable to the equation, in order to make the system adjustable, as follows:

$$Rx = T_x - T_xCable + T_xGain - fspl + R_xGain - -R_xCable + S \qquad (15)$$

E. Triangulation

Supposing there are 3 circles cutting each other, represented in Figure 5, with the relative positions of their centers represented as (x_A,y_A), (x_B,y_B), (x_C,y_C) respectively. Using (8), we can discover the distances of the F point from those 3 points, *dFA* ,*dFB* , *dFC*.

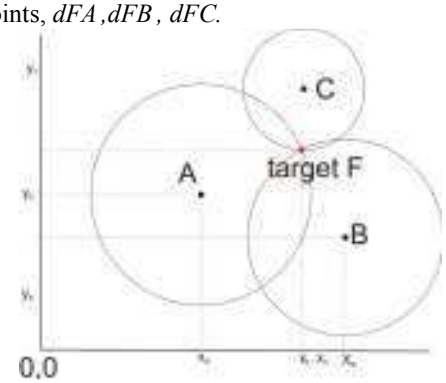

Figure 5: Three intersecting circles with target F

TABLE II. 3 WELL KNOWN SPOTS COORDINATES

	Point A	Point B	Point C
Distance from F	dA=dAF	dB=dBF	dC=dCF

If we represent the F point as a moving Wi-Fi station in a well known (x,y) area, using the known Euclidean equation of circle,

$$(x_i - x_F)^2 + (y_i - y_F)^2 = diF^2, i \in \{A,B,C\} \qquad (16)$$

three second-degree equations are formed.

Subtracted by factor they yield two one-degree equations with two unknowns (x_F,y_F). Those equations can be continuously calculated, with no significant needs of computational power.

VII. ARCHITECTHURE AND IMPLEMENTATION OF THE NETARGUS SYSTEM

The "NetArgus" application collects the available SNMP information from the network devices in order to construct the network structure and investigate its status.

NetArgus system is a 3-tier network application that operates over TCP/IP networks (Fig. 6). The system uses Microsoft SQL Server 2005 for data storage. The current version of the system runs under Microsoft Windows XP OS on client side and Microsoft Windows Server 2003 on server side.

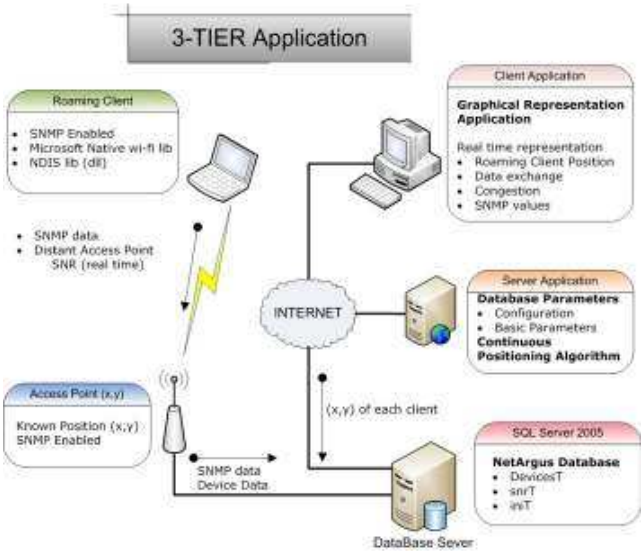

Figure 6: Application Created Model

The NetArgus system application is divided in three separate applications, which communicate using the common database and TCP/IP network messages. In detail:

A. NetArgus Client

This is the part of the software that is installed in the moving client's PC. It sends in real time the signal level of all the APs in its region thought the wireless network card. The collected information is stored in the database.

The application runs as a process in the background and it can be configured through a windows form (Fig. 7). NetArgus client also collects information about the AP's Mac Address, SSID, Security protocol, Network type, speed, etc. in order to inform the database with as much information as it can.

* *Paper Presented at IARIA - ICWMC 2009, at Cannes/La Bocca, France, winning the "Best Paper Award" price*

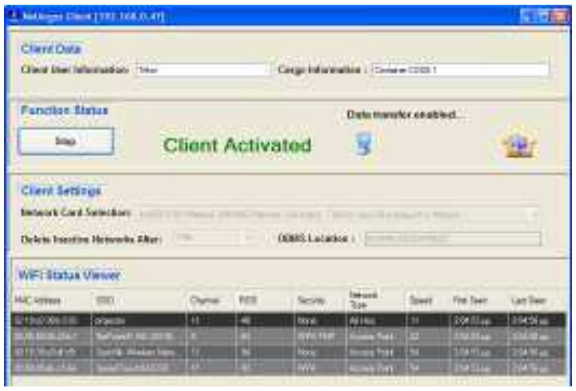

Figure 7: NetArgus Client

B. *NetArgus Server*

The second part of the application is the Server-side application (Fig. 8). It reads information from the moving client and using the triangulation algorithm described in VI.E, computes the absolute position of this client, storing that information into the database.

Figure 8: NetArgus Server

C. *NetArgus Viewer*

That is the graphical representation module that is used for presenting the network devices and the network structure on a map.

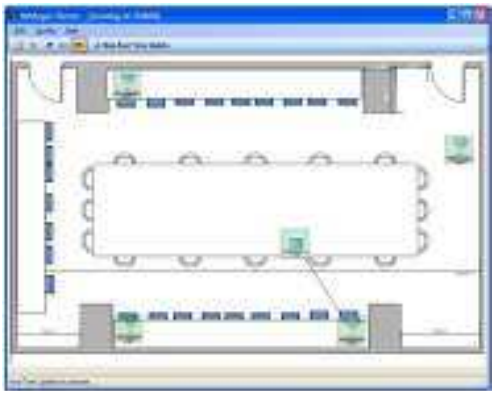

Figure 9: NetArgus Viewer, Classroom Tested

Moreover it shows in real time the movement of the mobile clients in the covered area (Fig.9).

That part of the application is independent. It can be anywhere with access to the main database anyhow e.g., through VPN. It gives a lot of configuration options in order to make the graphical representation as real as it can be. Any existing map can be uploaded, with a definable scale. Using a fully automated network device miner that uses SNMP, existing mobile clients and APs can be identified in a given network.

VIII. CONCLUSION

A three-tier distributed application was created, following all the modern design patterns.

The client applications (NetArgus Client & NetArgus Viewer) communicate with the NetArgus Server application, which can rely on a different location than the previous two. The positioning finding algorithms are running in real time here.

The NetArgus Client is installed in every moving station we care of finding its position. It continuously sends to the database the received Signal level from all the APs within its reach.

The NetArgus viewer is the GUI of the collected data. It communicates with the database, stating on a (user created) graphical map of the given area (x,y) the position of the moving station in real time with no significant overload. It also represents (possibly graphically) all the SNMP collected information from the network.

The application was tested in various harsh environments in real time. It did find the position of the station with a relative accuracy. Valuable results were gathered according to the quality of the received signal, the distance between station and the hardware used, specially the differences between various vendors.

A discovery was made, that there is a theoretical low boundary of the location finding accuracy. Because of the representation of the signal level as an integer and the logarithmic equation used, the transition from one integer to the next brings an error of at least 2.5 meters. This was not found documented in any relative work.

The application significantly deviates from its boundaries in close spaces, where it is obvious that noise exists. To address this problem, the addition of a Kalman filter [31], is the scope of a current under working essay.

According to SNMP, the application can easily accept changes and additions to the MIB used, representing graphically or not, the obtained information.

IX. FUTURE WORK

Regarding SNMP, various additions can be easily made, such as exporting results of routing loads of a network and the possible optimization through dynamic routing protocols (RIP, BGP, IGMP), or possible implementation of network watch applications e.g., clever water leakage sensors.

** Paper Presented at IARIA - ICWMC 2009, at Cannes/La Bocca, France, winning the "Best Paper Award" price*

Regarding the 802.11 protocols, there is a wide area open. This is the roaming protocol between the transmitting APs. The 802.11 protocol gives some general directions, but every manufacturer implements its own methods (most of the times without documentation) making the possibility of roaming between devices of different vendors, almost impossible.

The positioning finding algorithms can be improved and expanded specially on the direction of including smart devices such as telephones, active tags etc.

With a little effort, the applications implemented can be used for:

A. Triangulation for Finding the Physical Position of a Transmitting 802.11 Station

With the use of any kind of vector maps (e.g. Google Earth [32]), or any kind of DEM maps with Latitude & Longitude information (a very good one is [33]), measuring up the signal strength at three random spots (Fig. 10), we can determine the co-ordinates of the broadcasting station in question.

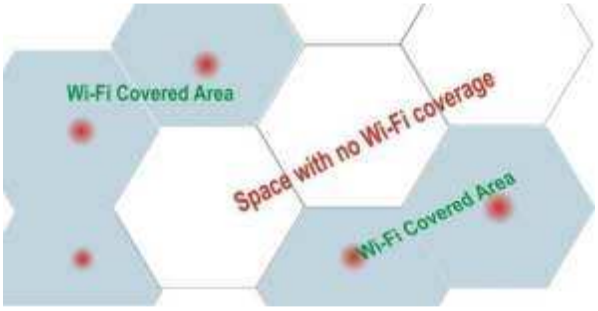

Figure 10: Empty space 802.11 signal coverage

B. Mapping and Tagging the Signal Level of all the Transmitting Surrounding Stations in a Given Space

The application implemented can also be used for the measuring of the signal level in a given area (Fig. 11), where several stations are broadcasting.

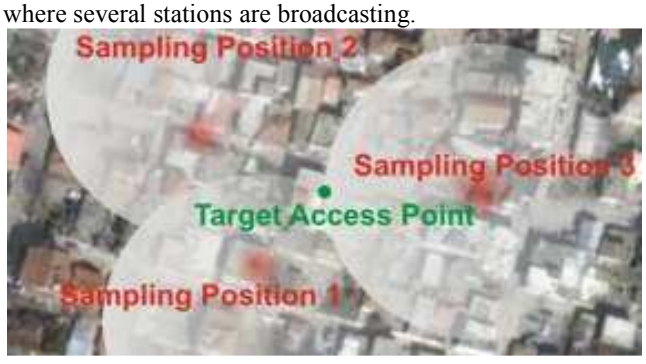

Figure 11: Triangulation of a known Target AP

This can lead to an optimization of the signal coverage through the physical re-location of the APs towards an optimum hexagon cell layout (the beehive effect in wireless networks [34]).

REFERENCES

[1] Cicso Systems, "Wi-Fi Based Real-Time Location Tracking: Solutions and Technology," 2006.

[2] "AeroScout," *Solutions Overview*.

[3] Ekahau, "Real Time Location System (RTLS) Overview."

[4] Interlink Networks, "A Practical Approach to identifying and Tracking Unauthorized 802.11 Cards and Access Points," 2002.

[5] Paramvir Bahl, Venkata N. Padmanabhan, and Anand Balachandran, "A Software System for Locating Mobile Users: Design, Evaluation, and Lessons," 2002.

[6] Antti Seppänen, Jouni Ikonen, and Jari Porras, "EXTRACTING AND USING POSITION INFORMATION IN WLAN NETWORKS."

[7] Antti Kotanen, Marko Hännikäinen, Helena Leppäkoski, Timo D. Hämäläinen, "Positioning with IEEE 802.11b Wireless LAN."

[8] Douglas Mauro, Kevin Schmidt, *Essential SNMP | O'Reilly Media*, O' Reiily, 2005.

[9] D. Harrington, R. Presuhn, B. Wijnen, "RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," Dec. 2002.

[10] Wikipedia, "List of WLAN channels," *List of WLAN channels*.

[11] IEEE, "IEEE 802.11 Official Timelines," *WORKING GROUP PROJECT TIMELINES*, 2008.

[12] James F. Kurose, Keith W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison Wesley, 2000.

[13] Vaughan-Nichols, S.J. , "The challenge of Wi-Fi roaming," pp. 17- 19.

[14] IEEE, "ANSI/IEEE Std 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Edition. 1999.

[15] Microsoft MSDN, "MSDN 2.2.1.1.13 802.11 RSSI," 2008.

[16] Microsoft, "WMI Overview," *Microsoft Windows 2000 Scripting Guide*, 2008.

[17] Microsoft MSDN, "Networking Developer Platform Center," *Native Wifi (Windows)*.

[18] Microsoft Developer Network , "WMI MSNdis_80211," *ServiceSetIdentifier query returns garbage*.

[19] Microsoft Developer Network, "Forums," *how can i get visual basic to scan for wireless networks?*, 2007.

[20] "NDIS Developer's Reference," *What is "NDIS"?*, 1996.

[21] "Clemson Vehicular Electronics Laboratory," *Working with Decibels*.

[22] J.H. Winters, "Smart antennas for wireless systems," *Personal Communications, IEEE*, 1998, pp. 23-27.

[23] Theodore S. Rappaport , *Wireless Communications Principles And Practice*, Prentice Hall Ptr , 2001.

[24] Yajun Kou , "Derivation the dB version of the Path Loss Equation for Free Space.," *Universtiy of Victoria*, Sep. 2000.

[25] Wi-Fi Alliance, "What is the range of a wireless network?," *Knowledge Center*.

[26] "Proxim Wireless," *Calculations: System Operating Margin (SOM)*, 2009.

[27] John Krumm, John C. Platt, "Minimizing Calibration Effort for an Indoor 802.11 Device Location Measurement System ," *Microsoft Research*, Nov. 2003.

[28] Rahul Tandra, "Fundamental limits on detection in low SNR," Master Thesis, University Of California, Berkeley, 2005.

[29] Consultative Committee for Units (CCU), "Report of the 15th meeting," Apr. 2003.

[30] Wild Packets Inc, "Converting Signal Strength Percentage to dBm Values," Nov. 2002.

[31] Greg Welch, Gary Bishop, "The Kalman Filter."

[32] Google, "Google Earth," 2008.

[33] Peter Guth, "MICRODEM Home Page," *Oceanography Department, U.S. Naval Academy*, Mar. 2007.

[34] Gordon L. Stuber, *Principles of Mobile Communication, 1st edition*, Norwell, MA, USA: Kluwer Academic Publishers, 1996.

** Paper Presented at IARIA - ICWMC 2009, at Cannes/La Bocca, France, winning the "Best Paper Award" price*