Geofencing Components and Existing Models

Anthony .C. Ijeh, David .S. Preston, Chris .O. Imafidon, Titus .B. Watmon, Annette .O. Uwaechie,
Aaron Nwadube, Ebrina Kujabi, *Member, IAENG*

***Abstract*-This paper describes the various Geofencing Components and Existing Models in terms of their Information Security Control Attribute Profiles. The profiles will dictate the security attributes that should accompany each and every Geofencing Model used for Wi-Fi network security control in an organization, thus minimizing the likelihood of malfunctioning security controls. Although it is up to an organization to investigate the best way of implementing information security for itself, by looking at the related models that have been used in the past this paper will present models commonly used to implement information security controls in the organizations. Our findings will highlight the strengths and weaknesses of the various models and present what our experiment and prototype consider as a robust Geofencing Security Model for securing Wi-Fi Networks**

***Index Terms* – Finger Print, Geofencing, Security Strategy Models, Radio Wave Propagation Models, Antenna, Wireless Fidelity, Location Estimation Models, Geolocation**

I. INTRODUCTION

Architecting security solutions for today’s diverse Wi-Fi network computer systems is a challenge. The modern business environment is comprised of many different applications, e-mail, databases, e-commerce, and more. Each of these has its own threat profile and associated business risk. The complexity of the computing environment extends to the design of security solutions. Current methodologies for designing security systems include piecemeal designs and patchwork systems comprised of multiple point solutions. The framework as shown in Figure 1 was used by **[1]** to show location based services at the intersection of GIS and other spatial technologies, the internet and the web, and new information and communication technologies (NICTs) As the complexity of the business driven systems increase, these methods are being strained to keep up with security requirements. Systems science provides information on how complex systems interact with their environment, and this guidance can be applied to designing security architectures. Analysis and design of security systems using systems theory provides a new path to reduce the complexity. As at the time of writing this paper we were not aware of any related work specific to our proposed models area which specifically relates to using Geofencing as a security strategy model **[2].** There are however several studies which have a relevant part in our project due to our projects nature of being made up of many components; these studies will be presented in this paper

II. EXISTING MODELS FOR GEOFENCING

In this section we present the techniques used both commercially and otherwise during the Geolocation process. The basic function of a Wireless Geolocation system is to gather particular information about the position of a Mobile Station (MS) and to also process that information to form a location estimate. The particular information could be in the form of the following: Received Signal Strength (RSS), Angles of Arrival (AOA), Times of Arrival (TOA) or Time Differences of Arrival (TDOA) as shown in Figure 2; Table II shows the accuracy that can be obtained in these models

III. RADIO WAVE PROPAGATION MODELS

The intensities of radio signals emitted from Wi-Fi networks can be used to detect the position of a mobile device due to the functional dependence between the received signal strength from an access point (AP) and the physical position of the mobile device. The reality is though that the propagation patterns of these radio signals are extremely complex and difficult to be mathematically modelled. Operation of Received Signals Finger print Geolocation Technique is based on 2 phases: a) Off-Line phase (Phase of data collection) or Learning phase consists of recording a set of Information (in a database) as a function of the user’s location covering the entire zone of interest, forming a set of Fingerprints**;** b) Real-Time phase (Phase of user’s position location) for specific Fingerprint Information is obtained from measured received signals and compared with recorded set of Fingerprints which are pre-stored in a database as shown in Figure 3

Each Fingerprint corresponds to Fingerprint information associated to a known user’s location; A Pattern Matching Algorithm is then used to identify the closest recorded information of the database to the measured one, thus defining the corresponding user’s location. The Microsoft Corporation developed the RF based system for locating and tracking

Manuscript received (January 1, 2010). This work was supported in part by a grant from the Worshipful Company of Haberdashers UK and the free use of a Location Based Service Laboratory owned by AireTrak Ltd based At Huntingdon in the UK

A .C. Ijeh was with RSM Tennon, LLP, UK. He is now an Information Security Researcher with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (Corresponding authors phone: +44(0)208-223-7778; e-mail: ijehanthony@yahoo.co.uk)

D .S. Preston is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (e-mail: d.preston@uel.ac.uk)

C .O. Imafidon is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (e-mail: c.o.imafidon@uel.ac.uk).

T .B. Watmon is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (e-mail: bt.watmon@gmail.com)

A .O. Uwaechie is with Zenith Bank PLC (e-mail: Annette.Uwaechie@zenithbank.com)

A. Nwadube is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (email: a.nwadube@uel.ac.uk)

E. Kujabi is with the University of East London, 4 – 6 University Way, London, E16 2RD, UK (email: e.kujabi@uel.ac.uk)

users inside buildings; the system is known as the RADAR system for indoor tracking

IV. STATISTICAL LOCATION ESTIMATION MODELS

As a reminder the main focus of this paper was not to bring new signal propagation models for location estimation or new algorithms such as triangulation. It is rather to propose a new method of securing Wi-Fi networks using location based services in the form of Geofencing Engineering. However we need to understand the existing methods of monitoring human activity and how these methods work. Previous researchers have used the Principal component analysis (PCA) and Independent Component Analysis (ICA) to recognise human activity by extracting features from threes acceleration sensors that they attached to a users belt **[3]** this procedure allowed them to monitor the movement of users. For the purpose of our paper we have adopted the indoor location estimation method previously used by researchers **[4].** The reason for this is that our experiment is not aimed at proving that location based services work or that they can be used to monitor mobile devices; so many researchers have done this in the past to great success**[5] - [13].** Our experiment is simply to show that the Wi-Fi network can be protected by the use of user's location using location based services (LBS). The authors of our adopted model **[14]** used a simple but functional approach, using the functional relationship between the position of a mobile device and raw RSSI measurements. The statistical estimations were applied in a live environment and produced the results in Table II

V. RELATIONSHIP BETWEEN EXISTING MODELS AND THAT PROPOSED IN THIS PAPER

An analysis using SWOT of existing Geofencing and Security Strategy Models was undertaken in order to compare them to the application and theoretical frameworks used in this papers experiment. For the purposes of showing the relationships we used the Time Difference of Arrival (TDOA) and the Risk Based Audit (RBA) Approach. Our reason for this is that the TDOA is commonly and widely used for location based services worldwide and so also is the RBA approach to developing a security strategy. It is thus appropriate for this paper to use them as the bench mark for showing the strengths and weaknesses of this papers suggested frameworks. We have compared both SWOT analysis for securing wireless networks using previous research methods and our proposed model using **Table III and IV**

As previously discussed in this chapter the related work in the area of indoor location estimation and security strategy models concentrated more on algorithms for the location estimation methods and security models respectively rather than deployment and maintenance with consideration for emerging technologies. This paper focuses solely on deployment and maintenance algorithms as a form of access control for Wi-Fi networks. From the previous sections in this chapter it can be seen that location estimation techniques in wireless networks have been proven to work even if it meant combining methods to improve accuracy and when complemented with the Risk Based Audit approach used by organisations to draft security strategy models a somewhat fit for purpose strategy is built. However the model did not come without weaknesses as can be seen in **Table 3** and as such we present a proposed security strategy model in **Table IV**

Our approach in using Security Strategy Models and positioning technology as a hybrid system to secure Wi-Fi Networks is very different to what has been used in the past and automatically models the structure of buildings like corridors and office areas in order to select parameters to be used in controlling access to Wi-Fi Networks. Most of the previous work done using positioning technology emphasises a client-based location model and raises privacy issues in location-based services. However due to the current nature of Wi-Fi networks and their risks the preference is for an infrastructure-based solution. The authors have presented the components of positioning technology commonly used by most wireless network users and administrators. The aim of reviewing the components was so that the devices with security strengths can be used to develop a security model that can determine its location for which positioning using the mobile user can be used to grant access to the network

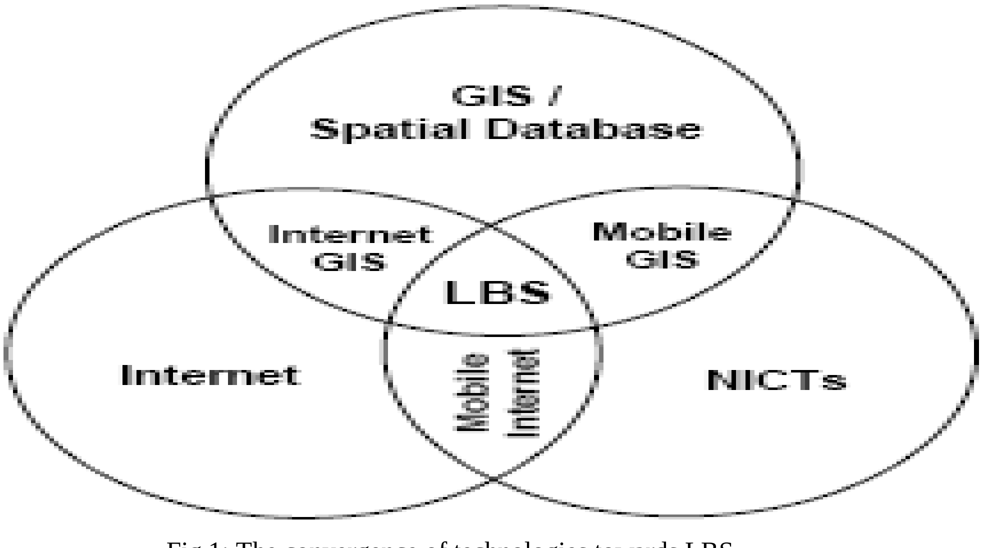


Fig 1: The convergence of technologies towards LBS

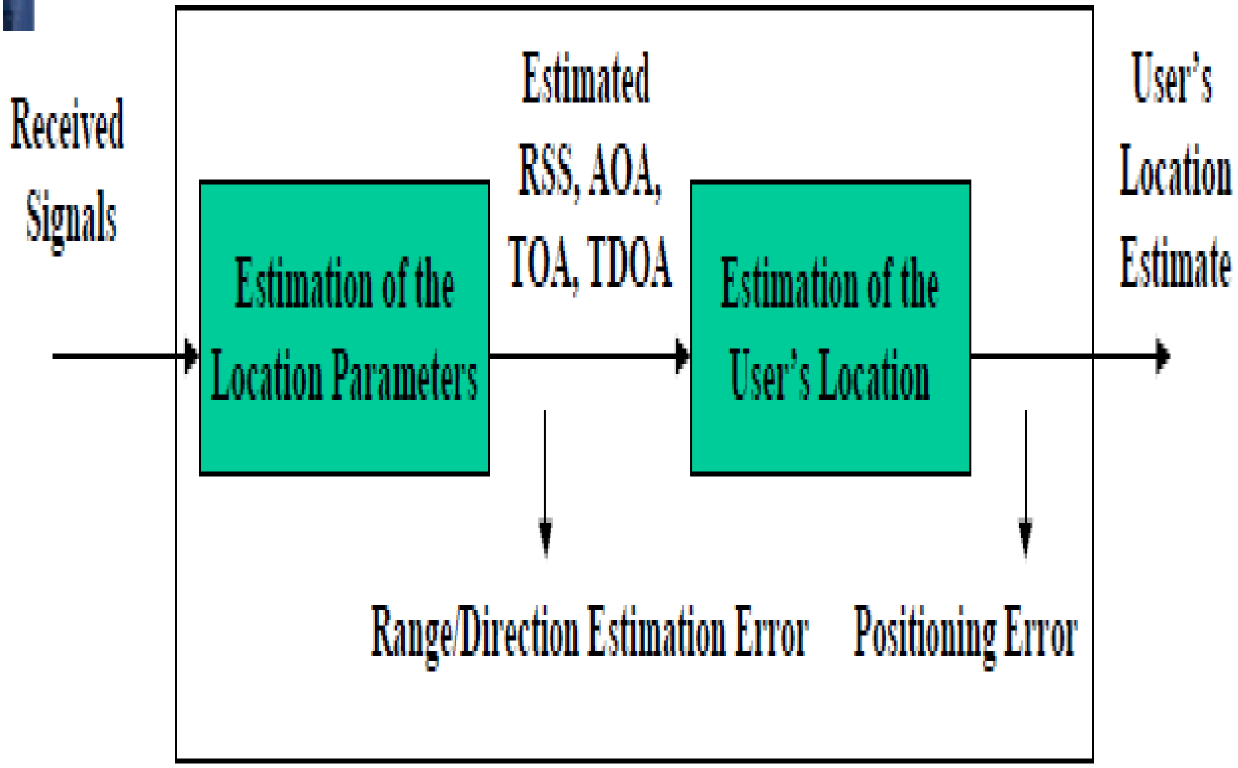
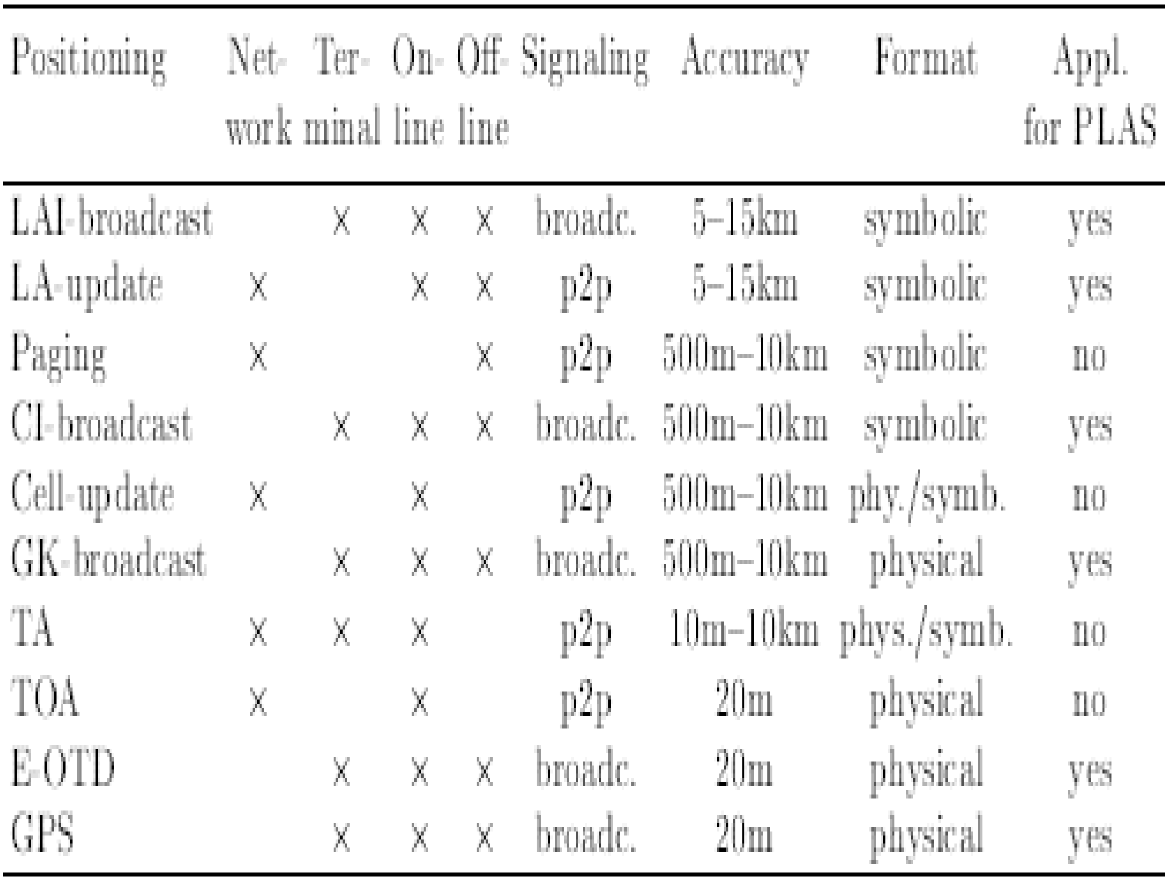

Received Signals
Estimation of the Location Parameters
Estimated RSS, AOA, TOA, TDOA
Estimation of the User's Location
User's Location Estimate
Range/Direction Estimation Error
Positioning Error

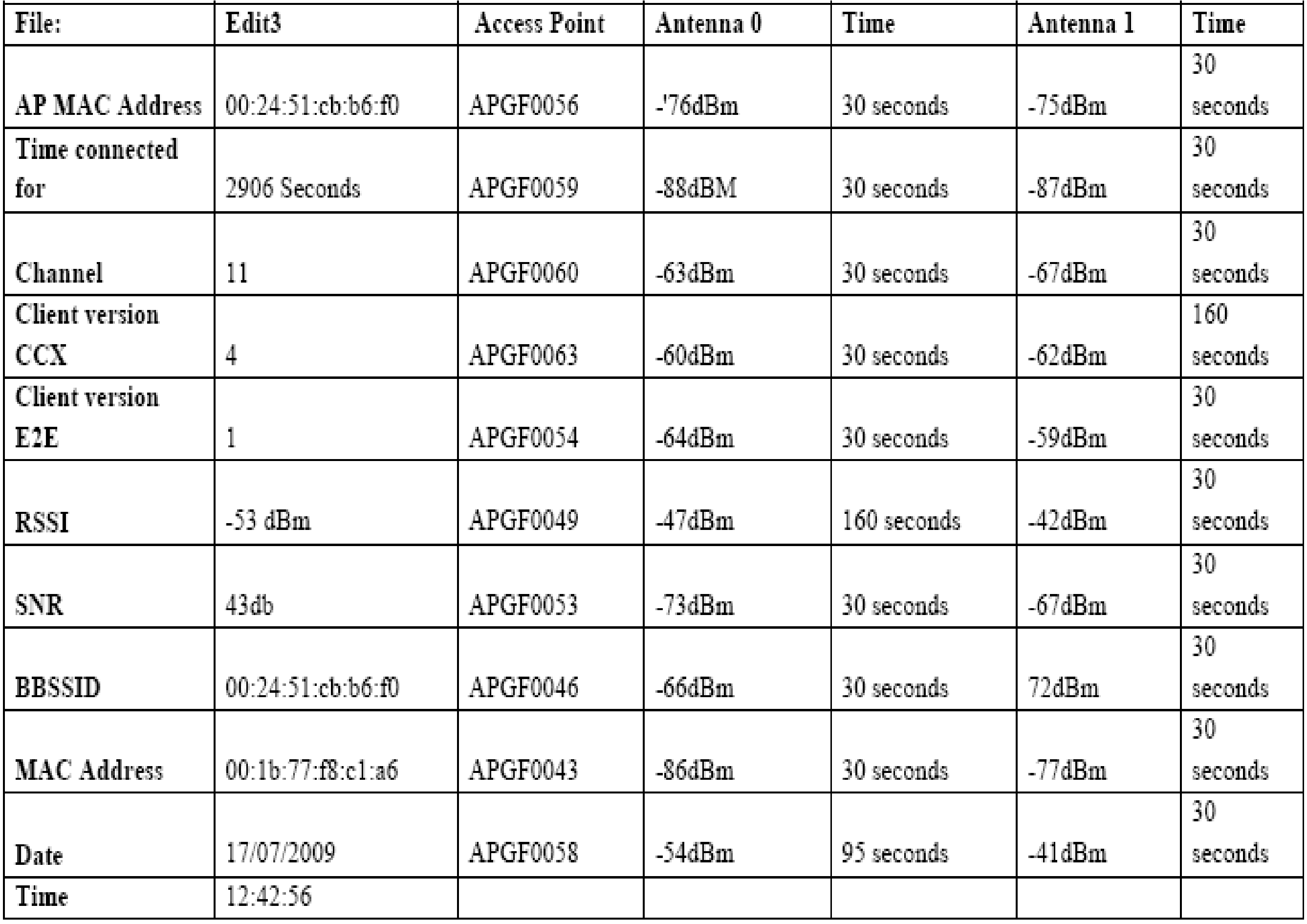
Fig 2: Geolocation Process

Table I: Accuracy in the Geolocation Process



Positioning	Network	Terminal	Online	Offline	Signaling	Accuracy	Format	Appl. for PLAS
LAI-broadcast		x	x	x	broadc.	5–15km	symbolic	yes
LA-update	x		x	x	p2p	5–15km	symbolic	yes
Paging	x			x	p2p	500m–10km	symbolic	no
CI-broadcast		x	x	x	broadc.	500m–10km	symbolic	yes
Cell-update	x		x		p2p	500m–10km	phy./symb.	no
GK-broadcast		x	x	x	broadc.	500m–10km	physical	yes
TA	x	x	x		p2p	10m–10km	phys./symb.	no
TOA	x		x		p2p	20m	physical	no
E-OTD		x	x	x	broadc.	20m	physical	yes
GPS		x	x	x	broadc.	20m	physical	yes

Table II: Results from our live Experiment showing part of a print off



File:	Edit3	Access Point	Antenna 0	Time	Antenna 1	Time
AP MAC Address	00:24:51:cb:b6:f0	APGF0056	-'76dBm	30 seconds	-75dBm	30 seconds
Time connected for	2906 Seconds	APGF0059	-88dBM	30 seconds	-87dBm	30 seconds
Channel	11	APGF0060	-63dBm	30 seconds	-67dBm	30 seconds
Client version CCX	4	APGF0063	-60dBm	30 seconds	-62dBm	160 seconds
Client version E2E	1	APGF0054	-64dBm	30 seconds	-59dBm	30 seconds
RSSI	-53 dBm	APGF0049	-47dBm	160 seconds	-42dBm	30 seconds
SNR	43db	APGF0053	-73dBm	30 seconds	-67dBm	30 seconds
BBSSID	00:24:51:cb:b6:f0	APGF0046	-66dBm	30 seconds	72dBm	30 seconds
MAC Address	00:1b:77:f8:c1:a6	APGF0043	-86dBm	30 seconds	-77dBm	30 seconds
Date	17/07/2009	APGF0058	-54dBm	95 seconds	-41dBm	30 seconds
Time	12:42:56					

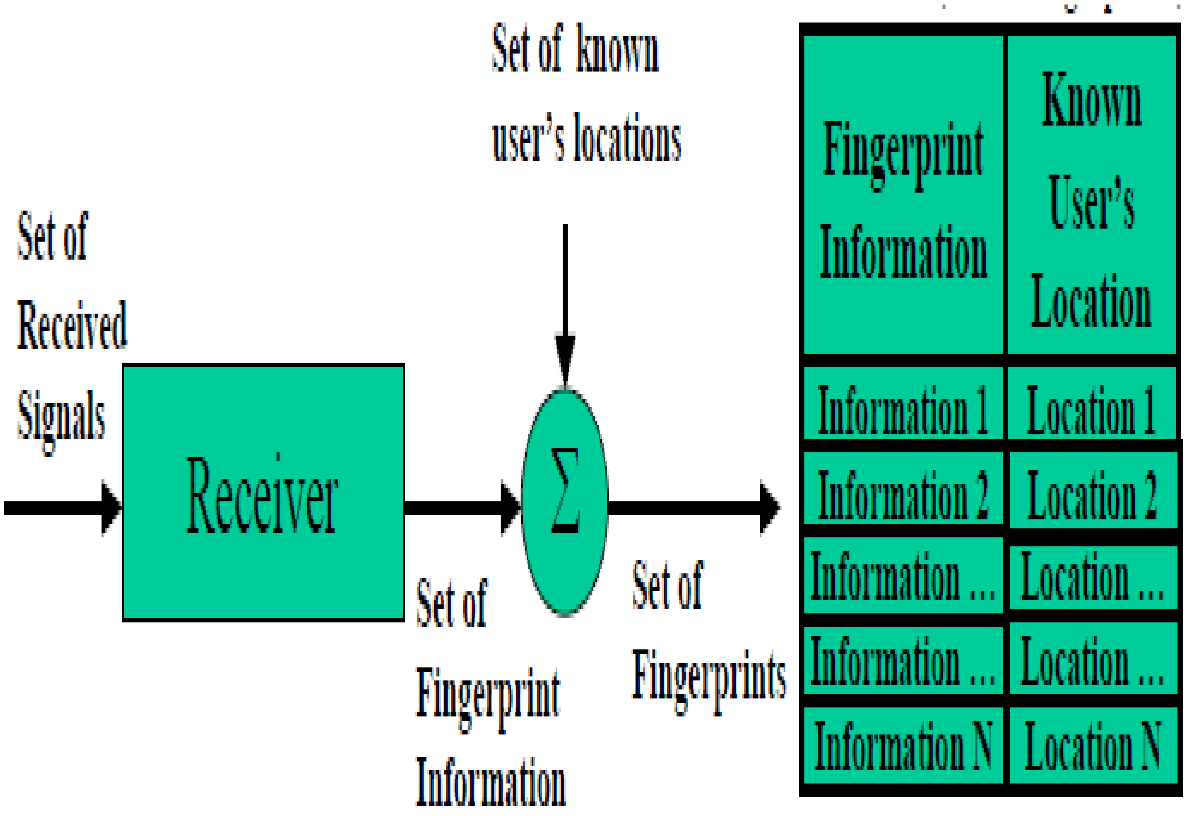


Fig 3: Received Signals Finger print Process

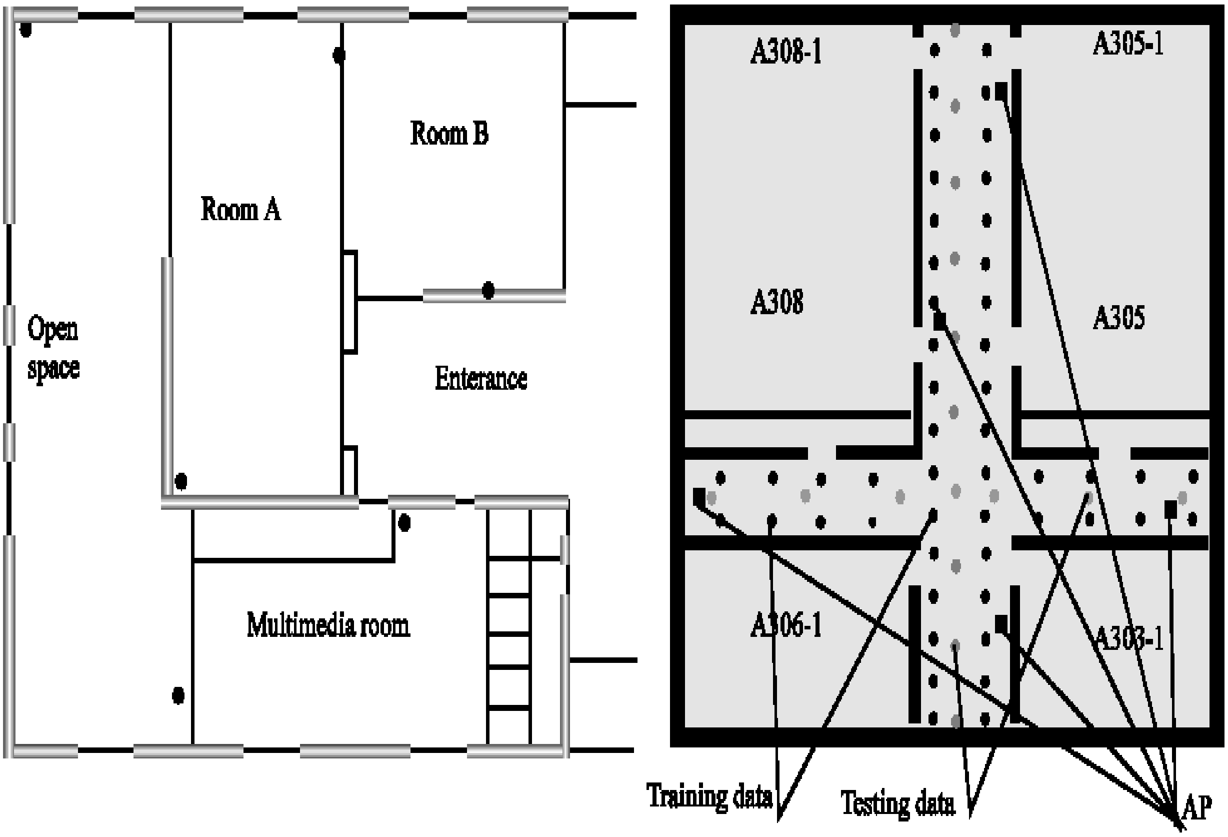
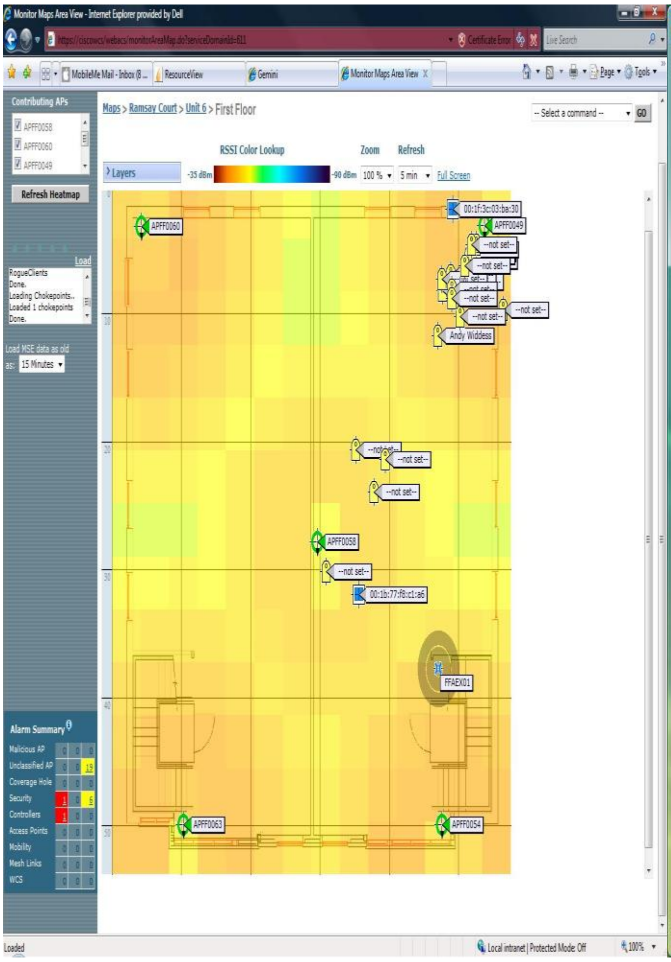
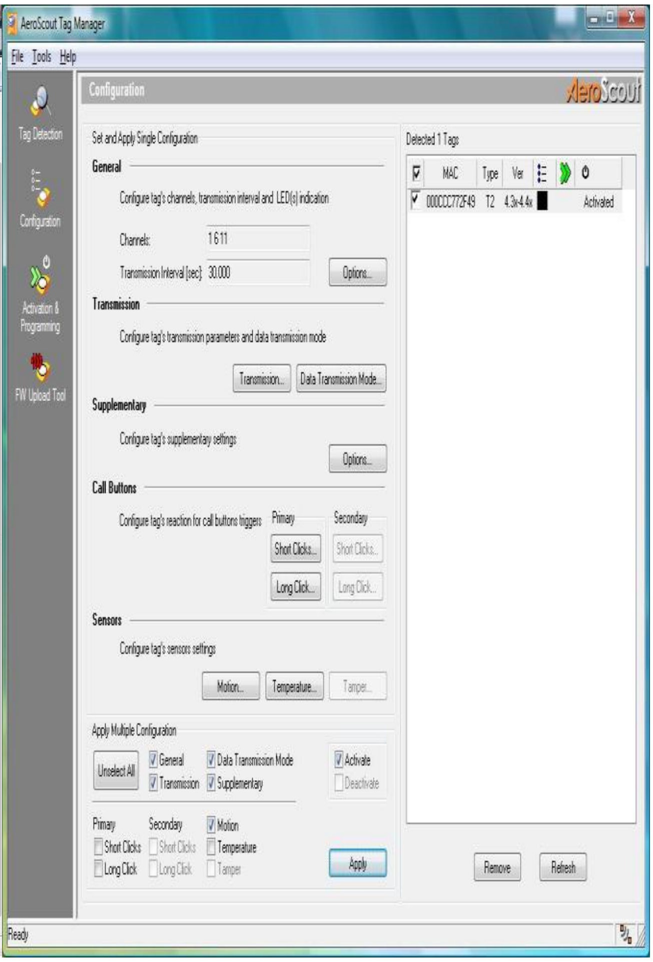


Fig 4: Test bed used by other authors & adopted as our location estimation method





Configuration

Set and Apply Single Configuration

General

Configure tag's channels, transmission interval and LED(s) indication

Channels: 1 6 11

Transmission Interval [sec]: 30.000 Options...

Transmission

Configure tag's transmission parameters and data transmission mode

Transmission... Data Transmission Mode...

Supplementary

Configure tag's supplementary settings

Options...

Call Buttons

Configure tag's reaction for call buttons triggers

Primary: Short Clicks... Long Click...

Secondary: Short Clicks... Long Click...

Sensors

Configure tag's sensors settings

Motion... Temperature... Tamper...

Apply Multiple Configuration

Unselect All ☑ General ☑ Data Transmission Mode ☑ Activate
☑ Transmission ☑ Supplementary □ Deactivate

Primary: □ Short Clicks □ Long Click

Secondary: □ Short Clicks □ Long Click

☑ Motion □ Temperature □ Tamper

Apply

Detected 1 Tags

☑	MAC	Type	Ver			
☑	000CCC772F49	T2	4.3x-4.4x	■		Activated

Remove Refresh

Ready

Fig 5: Test bed showing Access Points

Fig 6: RFID Tag configuration

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table III: Existing Security Strategy Models for Wi-Fi Networks

Strengths	**Opportunities**
Recognised by the International Standards Organisation (ISO) and the IEEE organisation	Trust model that takes into consideration the threat model and mitigates its risks. Emerging technologies means that the risks to the Wi-Fi network can be mitigated against in addition to encryption used to prevent clear text showing
Weaknesses	**Threats**
Does not take into account the leakage of radio waves used by the wireless network to transport confidential data which can permeate through building windows, doors and walls. The security strategy model is usually only recognised until the next protocol is released	Software Quality Wi-Fi Model structure Ethical Issues for using Wi-Fi Networks Wi-Fi Security Issues, including emerging threats IT Governance Standards for Wi-Fi Wi-Fi Protocol Compatibility of the components used in the Location Based Service Models and Security Strategy Models to provide security for the organisations data

Table IV: Proposed Security Strategy Model for Wi-Fi Networks

Strengths	**Opportunities**
Supports the use of encryption in securing Wi-Fi networks	Possible adoption as an ISO or IEEE standard
Weaknesses	**Threats**
Does not take into account the legal differences of different countries or their ICT standards which differ from country to country.	RFID propagation – Noise interference Wi-Fi Networks – varying protocols LBS Controller System - Compatibility Mobile Device e.g. Laptop - Configuration

References

[1] G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] Brimicombe, A.J., (2008) Location-based Services and GIS; In Hand paper of Geographical Information Science (edition J.P Wilson and A.S. Fotheringham), Blackwell, Oxford, 581 - 595

[3] Ijeh A.C; Preston, D.S; Imafidon, C.O (2009) “Geofencing in a Security Strategy Model” ICGS3’09 (formerly ICGeS) Conference Proceedings 1st to the 2nd of September 2009 www.springerlink.com/index/p85j16w581444106.pdf

[4] Mantyjarvi, J., Himberg, J., and Seppanen, T., (2001) “Recognizing Human Motion with Multiple Acceleration Sensors”

[5] M.C Su et al (2008) “A Regression –Model Based Approach to Indoor Location Estimation” IN the Journal of Engineering and Applied Sciences 3 (4): 307 – 311, 2008

[6] Brunato, M and Brunatti, R (2004) “Statistical learning theory for locating fingerprinting in wireless LANs” IN Elsevier Science

[7] Gwon et al (2004) “Robust indoor location estimation of stationary and mobile users” IN INFOCOM, 23rd Ann Joint Conference, IEEE Computer, Communication, Soc., 2: 1032 - 1043

[8] Hashemi, H (1993) “The indoor radio propagation channel” IN the proceedings of the IEEE, 81 (7): 943 - 968

[9] Li et al (2000) “Indoor Geolocation using OFDM Signals in HIPERLAN/2 Wireless LANs” IN the 11th IEEE international symposium, Personal Indoor and Mobile Radio Communication, 2: 1449 - 1453

[10] Mauve, M.A et al (2001) “A survey position-based routing in mobile ad hoc networks” IN the IEEE network, 15 (6): 30 - 39

[11] Niculescu, D (2004) “Positioning in ad hoc sensor networks” IN IEEE Network, 18 (4): 24 - 29

[12] Orr R.J. and Abowd G.D (2000) “The smart floor: A mechanism for natural user identification and tracking” IN the proceedings of the 2000 conference on Human factors in computing systems (CHI 2000), ACM Press, New York

[13] Pahlavan, K, X et al (2002) “Indoor Geolocation Science and Technology” IN the IEEE, Communication Magazine, 40: 112 - 118

[14] Patwari N.J.N et al (2005) “Locating the nodes: Cooperative localisation in wireless sensor networks” IN the IEEE Signal Processing Magazine, 22 (4): 54 – 68

[15] M.C Su et al (2008) “A Regression –Model Based Approach to Indoor Location Estimation” IN the Journal of Engineering and Applied Sciences 3 (4): 307 – 311, 200