Location Privacy of
Wireless Local Area Network Users
Using Client Server Based Architecture

By

Muhammad Junaid Khan

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Pakistan in partial fulfillment for the requirements of MS in Information Security

February 2012

ABSTRACT

In this advance technology world communication can now easily be done via wireless communication infrastructure. Now users can easily avail communication services even while roaming into different places.

Through the use of wireless communication infrastructure many of the techniques have been adopted to facilitate its users which include transmission security, voice and video services, user location identification etc. Due to advance researches and development in the wireless domain, location of any wireless user can now be collected using advance wireless location tracking techniques. There are so many such applications which are helpful providing user; information about different locations around them (i.e. restaurants, hotels, sport club, bar, masjid, market) however there are cases where it is necessary to protect the users location information from being used for some criminal activity.

There are so many techniques have been adopted to prevent user location information from being collected such as dynamically changing the interface identifiers, manipulating the received signal and time values, so as to obfuscate the attacker in long term movements.

This research discusses a technique through which user's location information can be altered so as to obfuscate the attacker. In this technique a middleware system that is carrying the record of all the RSSI (Received Signal Strength Identifier) values of each Wireless User connected to it sends the manipulated RSSI value to a source that is requesting for a location of WLAN / WCAN Users within its signal space.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

WLAN	Wireless Local Area Network
WCAN	Wireless Campus Area Network
AP	Access Point
LWAP	Lightweight Access Point
LWAPP	Lightweight Access Point Protocol
WLC	Wireless LAN Controller
RADIUS	Remote Authentication Dial In User Service
RSS	Received Signal Strength
RSSI	Received Signal Strength Identifier
BSS	Basic Service Set
BSA	Basic Service Area
ESS	Extended Service Set
LBS	Location Based Services
NLBS	Nearby Location Based Services
GSM	Global System for Mobile Communication
BTS	Base Transmission System
TOA	Time Of Arrival
AOA	Angle Of Arrival
TDOA	Time Difference Of Arrival
E-OTD	Enhanced Observed Time Difference
RFID	Radio Frequency Identification
LBS	Location Based Services
DMAS	Dynamic MAC Assignment with Shuffle
PDA	Personal Digital Assistance
IOS	Integrated Operating System
AES	Advance Encryption Standard

WPA	Wi-Fi Protected Access
LDAP	Lightweight Directory Access Protocol
CAPWAPP	Control And Provisioning of Wireless AP Protocol
NVRAM	Non Volatile Random Access Memory
POE	Power Over Ethernet
DHCP	Dynamic Host Control Protocol

Chapter 1

Introduction

1.1 Overview

Since the WLAN standard (802.11) arrived in the IT world, users everywhere from anywhere can easily use wireless services. All devices that are portable such like notebook / netbooks, handheld (IPods, IPads, smartphones and personal digital assistants) are nowadays comes up with built-in WiFi adapters and due to these WLAN / WCAN Interfaces there is a huge requirement of such services and application that can use Location Information with the help of several systems carrying several techniques of Location Detection of users having WLAN built-in devices.

If there is no user of sharing location information with anyone then there will also be no need to prevent individual user information from being collected for any criminal activity. Fortunately or Unfortunately users have to share the information as per their need via several services and applications which allures them to share their location information data mainly in case of navigation services , vehicle detection systems , product tracking , tourist guides, billing services on roads and tolls , advertisement alerts, social networking like locating friends and instant messaging etc. Talking about the disadvantages of the Location Detection, this technique does not only endanger users with traffic analysis attack but due to the information which resides on the servers that are mostly vulnerable the attacker can easily compromise them and then a user whose location information stored on the server can be suspected to computational privacy attacks, manual surveillance and hacking around different standard protection schemes.

1.2 Need for Research

Most of the time users share their location information unknowingly that such information can be misused against them but just due to such services and applications that allure them to share their location information they enhances their chances to be a victim due to some criminal activity by an attacker. There is an urgent need to emphasize the importance of protecting the location information owing to the

fact that the most potent attacks concerned to the location information by an attacker can be initiated using such information and they can be most of the time very dangerous such like if an attacker have all the information of when and where someone visits or changes his location regularly at the same time then he can easily prepare to attack that person or can commit crime such like robbery, attack someone's family etc. at the place someone live. In the context of Location Detection, the high degree of importance can be associated with the protection of user's location information from an adversary having access to the database server having huge repository of several users location information because if an adversary has all such then he can easily plan for any crime which is specific to the user location information.

1.3 Problem Statement

The current Client Server Based WLAN Location Detection Architecture does not guarantee the location privacy of WLAN / WCAN users [1]. The location information of the user either its is stored at some central location / vulnerable server or collected on real time basis can be used for deriving meaningful information about WLAN / WCAN users daily basis locations, hobbies, visit places. Collecting such information can provide an adversary several opportunities to generate several kind of attack which are more concerned to their physical location. To avoid the WLAN / WCAN user from being detected and to prevent their location information within the WLAN / WCAN signal space it is necessary to develop a technique that can ensure the privacy of WLAN / WCAN user location information. The technique should posses the incorrect information of the WLAN / WCAN user so that no one can infer the actual location of the user even if he detect the user within the WLAN / WCAN on real-time basis.

1.4 Objectives

This research work intends to highlight the importance of Location Privacy. It aims to develop the concept of preventing location information and to not to share them to avoid being attacked. In this research the major objective is to develop such a technique through which a WLAN / WCAN user can prevent sharing location information easily without the installation of any add-on application on his/her owned WLAN equipped device. This technique not only prevents from gathering actual user's location information but even if an adversary compromises the system storing

the location information cannot easily track the actual behavior of changing locations of an individual user. The ideology of the developed technique using appropriate methods of location detection and prevention harmonizes the researches' objectives.

1.5 Research Methodology and Achieved Goals

The research work was divided into three main phases. The phase 1 comprised of detailed study and reviews of existing literature on WLAN location detection architectures and also thoroughly reviewed them. In phase 2 of the research, the deployment of client server based architecture. During this phase, the traffic behavior of wireless user has been observed with the detail of information exchanged and flows between source and destination. The phase 3 included the comprehensive study of research domains closely related to this research work. During this phase, design goals were outlined for the development of an appropriate technique and WLAN user location detection attributes were analyzed with respect to how information exchanges in order to locate the WLAN user in client server based WLAN user location detection architecture. The individual components of proposed technique were designed, applied on client server based architecture and analyzed with respect to the associated design goals.

1.6 Thesis Organization

This thesis report is organized into 6 Chapters. Chapter 2: includes basic concepts of WLAN standards, types of WLAN deployment models and architectures, location detection and location privacy. Chapter 3: Discussion of WLAN location detection techniques, threats related to location detection. In this we also discussed the WLAN location detection architectures and the architecture used in this research whose components will be observed in order to implement the WLAN location privacy technique. Chapter 4: Includes related work. Outlines the design goals for the formulation of a suitable technique, the deployment of client server based WLAN location detection architecture [1] with construction of radio map and our proposed technique for preventing WLAN / WCAN user location information. Chapter 5: This will include the application of proposed technique on client server based architecture and will elaborate each of its phases, necessary to implement the technique. Chapter 6: Complete analysis of proposed technique and its comparison with selected already developed technique. Chapter 7: conclusion followed by a brief about future work.

Chapter 2

Overview of WLAN, Location Detection and Prevention

2.1 Introduction

This phase presents the basic concepts of WLAN standards and the deployment models and architectures. This phase also includes a brief explanation of location detection and different theories of experts in this ground. After the brief description of location detection we have also discussed the location prevention and its need along with the growing demand of location detection techniques / schemes.

2.2 WLAN Standards, Deployment Models and Architectures

After the successful implementation of wired infrastructure a new standard arrived that has the tendency to provide user numerous mobility services through a wireless connection, a standard that allows user to connect to the network without any physical connection and can have a freedom to work from anywhere while sitting anywhere within the Wireless signal space. This standard announced as Wireless LAN technology standard IEEE802.11. Due to its several advantages it becomes a main standard for corporate internal wireless LAN [2]. From number of its characteristics some of main are its simplicity, scalability and robustness due to its distributed architecture and shared medium [1][15][16][17][18]. IEEE802.11 has a family of four 802.11a/b/g/n all are different from each other with respect to the data rates 54/11/54/65-300 Mbps.

Mode	Channel	Streams	Peak Data Rate (Mbps)
802.11b			11
802.11a,g			54
802.11n (800 ns GI)	20 MHz	One	65
	20 MHz	Two	130
	40 MHz	One	135
	40 MHz	Two	270
802.11n with short GI (400 ns)	20 MHz	One	72.2
	20 MHz	Two	144.4
	40 MHz	One	150
	40 MHz	Two	300

Table 1: 802.11n Data Rates

WLAN has two types of deployment models:

Ad-Hoc Model – All wireless stations within the wireless communication signal space can interact with each other without having involvement of any central entity.

Figure 2.2(1): WLAN Ad-Hoc Model

Infrastructure Model – A central entity that is involved in the end to end communication between two or more than two hosts, all stations within the wireless communication space need to connect to that central entity and it has the responsibility to provide communication between all hosts in the same or different network. This central entity is names as Access Point.

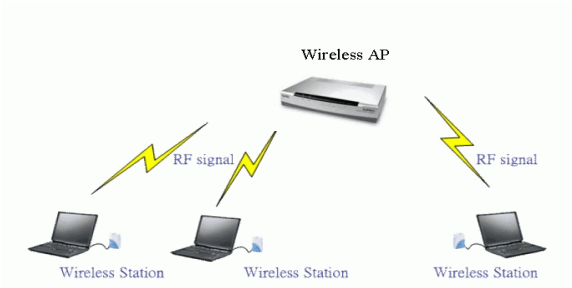

Figure 2.2(2): WLAN Infrastructure Model

IEEE802.11 has the two fundamental parts of its complete architecture which are BSS or BSA and the other one is ESS.

BSS – Basic Service Set is a collection of stations that are located in the same geographical area and in this each station within the same area can directly communicate with any other station without use of any central communication authority. This is also termed as BSA.

ESS – To form an extended service set there always be an involvement of Access Point that builds an infrastructure network and provides a geographical extension through which multiple BSS can be integrated together to form an ESS, and so any station that lies under one basic service area can communication with station that lies in another basic service area though the help of Access Point.

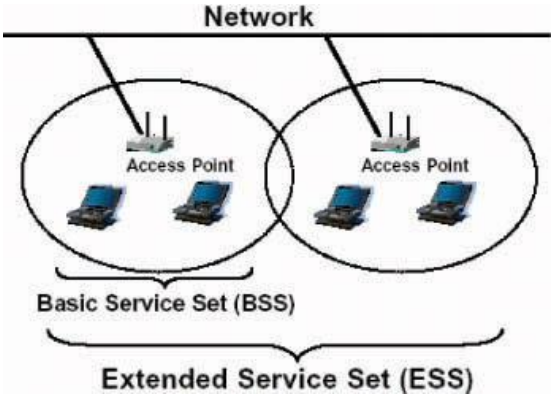

Figure 2.2(3): WLAN Architecture

2.2.1 Location Detection

Location detection comes from the use of LBS, LBS are information service which uses the actual or nearby location information of user in order to provide them different kind of facilities (i.e. nearby hotels, casinos, sports club, hospital, franchise etc.) it can be used in several other kind of contexts likewise for health, work, indoor searching of objects.

Location detection has become very popular and most demanding due to LBS. There are three types of location detection methods:

- Control Plane Locating
- GSM Localization
- Location Detection in NLBS

Control Plane Locating – Service provider receives the location information that is based on the delay in radio signal from the closest cell-phone tower. It is completely based on radio network with no GPS usage and that is why it has slow response.

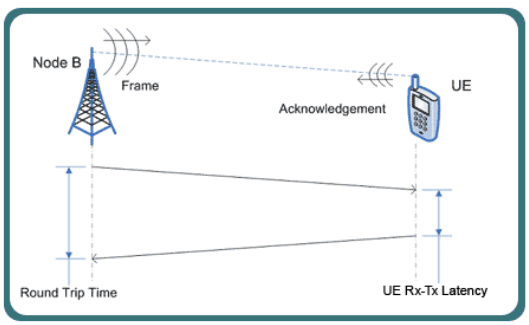

Figure 2.2.1(1): Control Plane Locating

GSM Localization – Method of extracting the location of a mobile device by using cell sites. Other effective method includes multilateration of signals from BTSs service mobile device, TDOA and E-OTD.

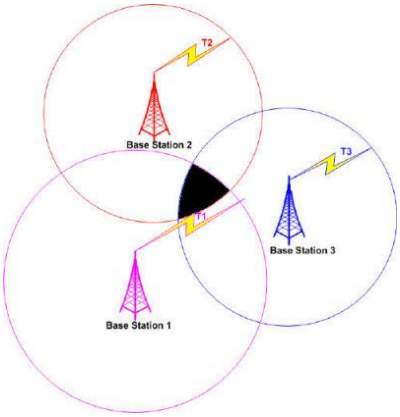

Figure 2.2.1(2): GSM Localization

Location Detection in NLBS – Method in which devices that has low range of signals as compare to the large radio networks and GSM networks are used to detect the user location within the small geographical or regional areas. This includes technologies like Bluetooth, Infrared / RFID / Near Field Communication and **WLAN.**

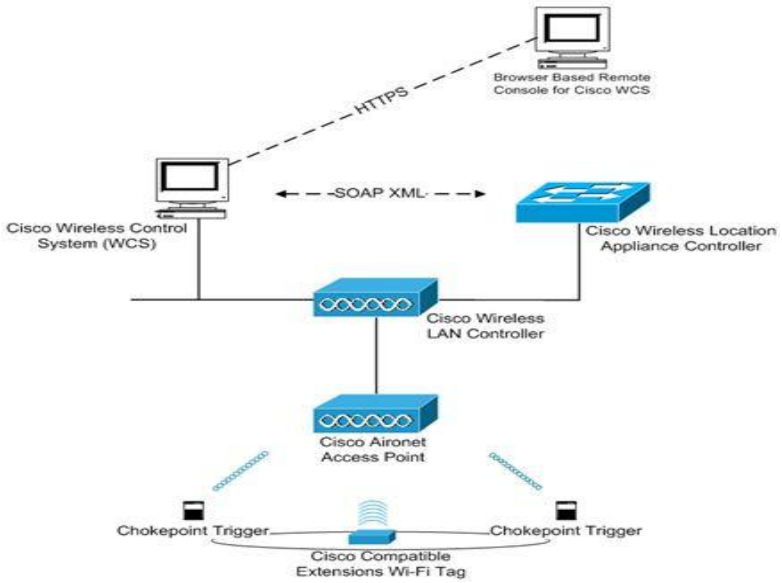

Figure 2.2.1(3): Location Detection in NLBS

2.2.2 Location Privacy

Day to day increasing need of location detection techniques in location based services enhancing the applications and services relevant to the user location information in the tech. market. This user location information resides on central server; any of such server that has vulnerability in it and is untrusted then the privacy of user location information and its security can be disclosed to any of the adversary or an attacker who can use such information to reveal person's political, religious and medical affiliations [3]. Due to this; privacy of user location information becomes more important than sharing the user location information in many of the cases and hence several papers and researches have been done to prevent sharing of user's actual location information. As the outcome of such researches there are three main architectures have been proposed which are:

- Client Server (Research uses this method)
- Trusted Third Party
- Peer Based

Client Server Location Privacy Architecture – In this model any untrusted party has the access to the server that is storing user's actual location information, the server then provides the obfuscated information of user's location to untrusted party requesting for the user's location [4] this will be the type of model which we have used in our research.

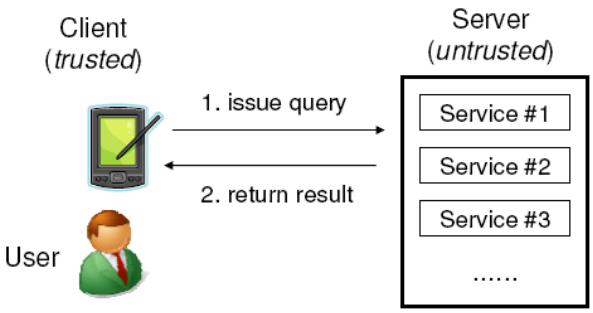

Figure 2.2.2(1): Client Server Location Privacy Architecture

Trusted Third Party Location Privacy Architecture – It involves a trusted third party who prevents the user's location information from being shared a good example is a GSM network based location privacy architecture or GPS based

architecture. A trusted authority implements a mechanism which prevents the user location information.

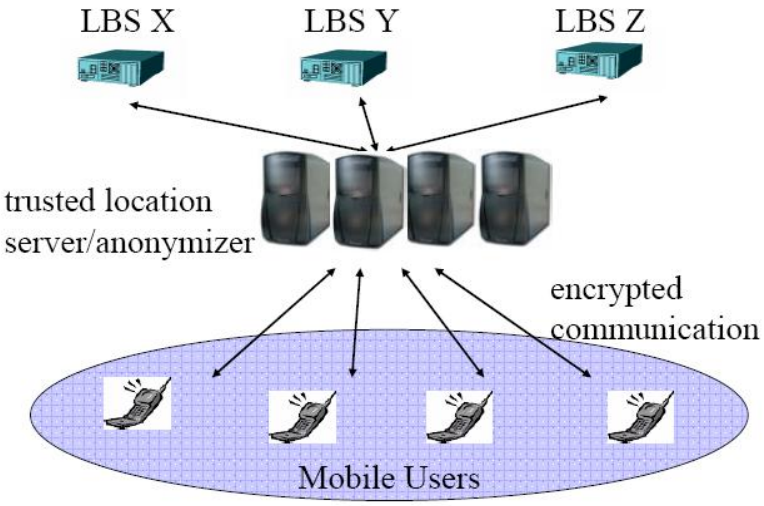

Figure 2.2.2(2): Trusted Third Party Location Privacy Architecture

Peer Based Location Privacy Architecture – This involves peer-to-peer based cloaking, in this each user communicated with its neighbor to discover peer locations hence it blurs the actual location information of users for the query initiator without using any central authority [5].

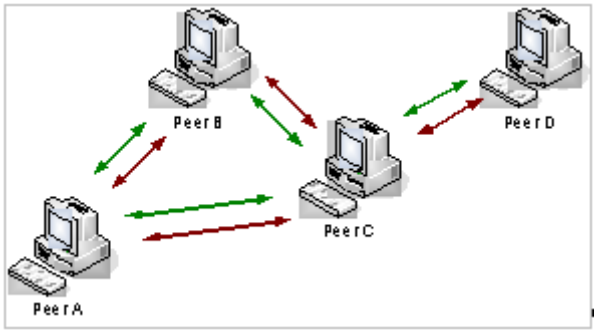

Figure 2.2.2(3): Peer Based Location Privacy Architecture

2.3 Summary

In this chapter we have discussed initially the WLAN standards and its available connectivity models. It also consist the study of all currently in use WLAN location detection architectures with the details of how they are related to location privacy requirement.

Chapter 3

WLAN Location Detection Techniques and Architectures

3.1 Introduction

Since the arrival of IEEE802.11 new generation wireless local area network provided a great freedom to user service of internet and local area network almost anywhere on regular basis. Nowadays there are so many handheld and portable devices that are carrying Wireless Enabled devices embedded (i.e. notebooks, netbooks, PDAs, Smartphones etc.). Due to this large number of devices with wireless interfaces there now a huge market for such services and application that can utilize the location information as provided by location detection system in contrast with users having WLAN equipped devices.

3.2 WLAN Location Detection Techniques

There are number of different kinds of positioning systems available for outdoor and indoor for determining location of any user. Some of examples are GPS, assisted GPS and cellular based network positioning systems that relies on several values / attributes. Surprisingly many of the system that discusses about location detection of user (indoor / outdoor) utilize almost same methods [6]. Techniques which are used in WLAN location detection are mentioned and we will briefly describe them:

- Time Of Arrival
- Time Difference of Arrival
- Angle of Arrival
- Received Signal Strength
- Location Fingerprinting

TOA Based WLAN Location Detection – This technique is based on the measurement of arrival time of signal propagation from a radio transmission device to one or more than one radio receiving devices. On the basis of arrival time an object can be estimated in terms of its distance from the receiver station.

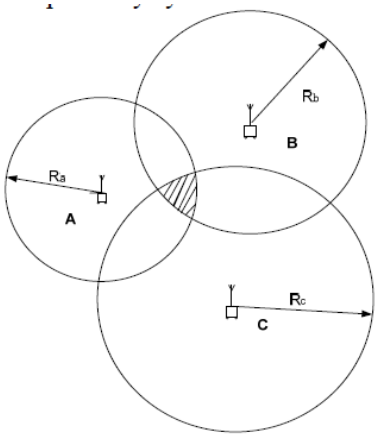

Figure 3.2(1): TOA Based WLAN Location Detection

TDOA Based WLAN Location Detection – This technique is an algorithm that is based on TOA technique which basically determines the object's distance by finding the differences of the TOA from transmitter to several receivers. The minimum measured difference in sets of different receivers with a transmitter quantifies the lower proximity of the transmitter with one of the receiver.

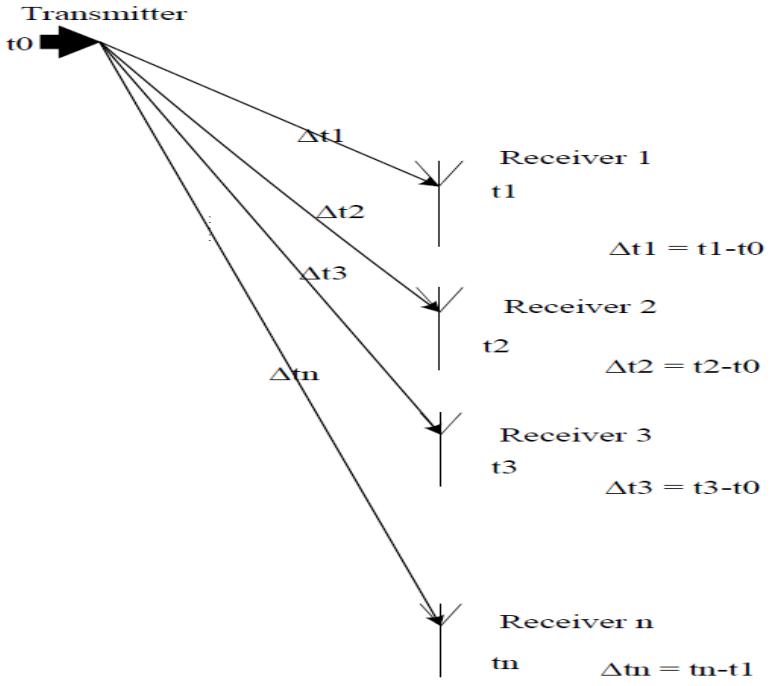

Figure 3.2(2): TDOA Based WLAN Location Detection

AOA Based WLAN Location Detection – This technique is widely used in wide area WLAN / WCAN. This technique determines the user location by measuring the angle at which the signal has been received from the transmitter. Larger the angle more far the object is, smaller the angle is the closer the object is.

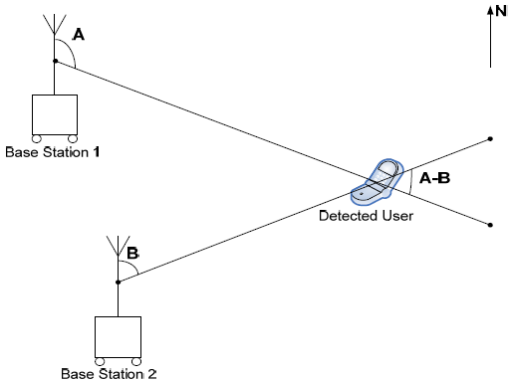

Figure 3.2(3): AOA Based WLAN Location Detection

RSS Based WLAN Location Detection – This technique is bit complicated but also widely used. It measures the magnitude of electrical signal that is collected at the receiving point. In this the power that is emitted to the transmitter is constant or always known to the receiver at the receiving end, the measured difference between the electrical signal value that is transmitted and is received at the receiving point identifies the distance of the object from the receiver.

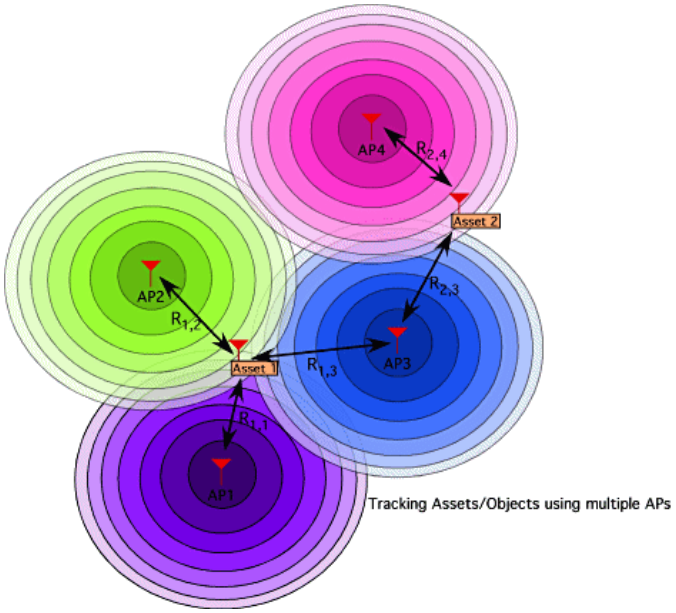

Figure 3.2(4): RSS Based WLAN Location Detection

WLAN Location Detection by Location Fingerprinting– This technique uses the above defined techniques and obtains collection of fingerprints of the object on the basis of which it drives the other relevant location information about the object. This technique uses the above techniques altogether to obtain accurate data about user's visited locations.

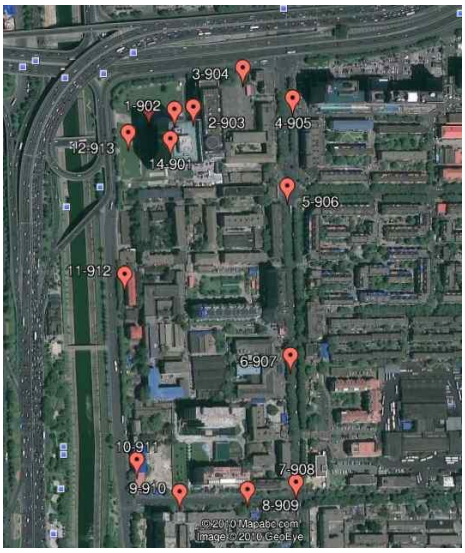

Figure 3.2(4): Fingerprinting WLAN Location Detection

3.3 Threats relevant to LBS uses Location Detection Techniques

It is a right of any individual, group of people or of any institution to identify that what information or up to what extent the location information should be shared with others. Through location detection of services that works on location detection techniques names as location based services can easily provides learning path towards any individual's or group's current and past location information. For this a term knows as location privacy introduced with several techniques that has the ability to prevent other parties from learning's one's location information [7]. Threats that are relevant to LBS are:

- Communication privacy threats
  - Sender's anonymity
- Location inference threats
  - Precise location tracking
  - Observation identification

- Restricted space identification

- Anyone can learn user's alternative lifestyles, medical conditions, can drive political and religious reviews.
- Stalking, domestic abuse and physical harm etc.


http://www.foxnews.com/story/0,2933,131487,00.html

FOX NEWS .com

U.S. & WORLD

Updated: 3:28:08 9:42pm ET

SEARCH GO

E-MAIL STORY PRINTER FRIENDLY FOXFAN CENTRAL

Man Accused of Stalking Ex-Girlfriend With GPS

Saturday, September 04, 2004
Associated Press

GLENDALE, Calif. — Police arrested a man they said tracked his ex-girlfriend's whereabouts by attaching a global positioning system (search) to her car.

Ara Gabrielyan, 32, was arrested Aug. 29 on one count of **stalking** (search) and three counts of making criminal threats. He was being held on $500,000 bail and was to be arraigned Wednesday.

"This is what I would consider stalking of the 21st century," police Lt. Jon Perkins said.

Figure 3.3(1): Example of Threats to Location Detection

3.4 WLAN Location Detection Architecture

WLAN infrastructure can be made more efficient without any additional hardware resource by just using the WLAN location architecture [1]. Researchers have developed architectures [1.6][1.8] in order to achieve the different level of efficiency of WLAN, below are the brief details about each of the architecture:

- Source-Destination Architecture
- Client-Server Architecture
- Sniffer Based Architecture
- Access Point Based Architecture

Source-Destination Based Architecture – This architecture provides user (source) to search any other user (destination) in the same BSS or any other BSS. One user can have the reachability to another user (destination) either it's of same network or of other network via destination that has connectivity to the actual destination in the WLAN. The connecting destination between source and actual destination records the RSSI values of the actual destination and on the basis of record RSSI of actual destination, its location can be found using radio map.

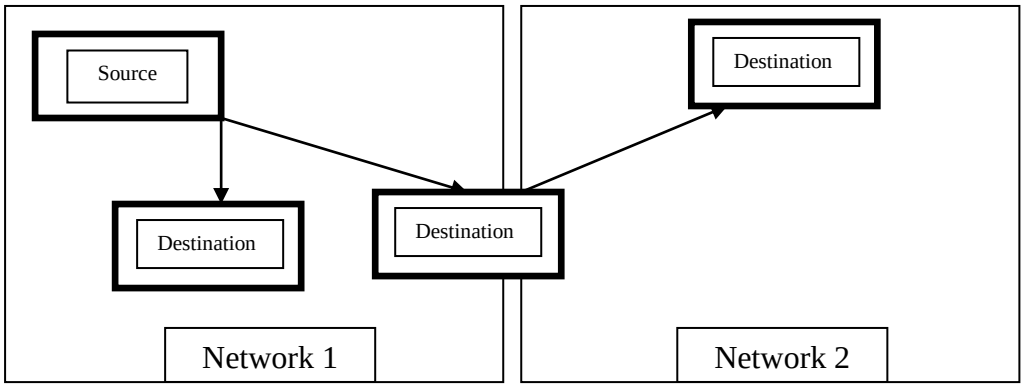

Figure 3.4(1): Source-Destination WLAN Location Architecture

Client Server Based Architecture – This architecture is composed of two phases of location estimation:

Offline Phase – In this phase the WLAN infrastructure mode's AP provides services to all the clients in the area as an ESS. In an ESS there are many APs and the client under the signal space of one AP can receive the signal from other AP too but only one AP has to server that client and that decision is made by client through the RSSI from other APs.

Real-time Phase – In this phase when the client initiates the requirement of the service that is then made available to the AP that is closest to that client using LBS.

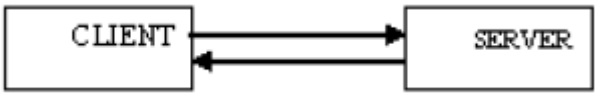

Figure 3.4(2): Client Server Based WLAN Location Architecture

Sniffer Based Architecture – This architecture is application based architecture and an application which is installed on all the system in the WLAN determines the

location of the system. This application software monitors the traffic from all the stations in the network. This application is called Sniffer in the network. In order to record all the WLAN traffic including the RSSI values of WLAN clients WNIC are used. Complete process includes two methods used by Sniffer in which first is detecting the RSSI values of all the clients in the WLAN (ESS) network, secondly recording RSSI differences from more than one reference devices (Sniffer (system with WNIC and application)), construction of locating model in the map.

Figure 3.4(3): Sniffer Based WLAN Location Detection Architecture

AP Based Architecture – This architecture uses the ESS architecture of WLAN and also the use of RADIUS server that is associates with each of the AP in an ESS and it stores all the information of the clients that are associated with their respective APs so that if a client wants to connect to any remote station then its parent AP contacts the RADIUS to find the location of that remote station [1.1] and the RADIUS replies that AP with the required available information of the remote station.

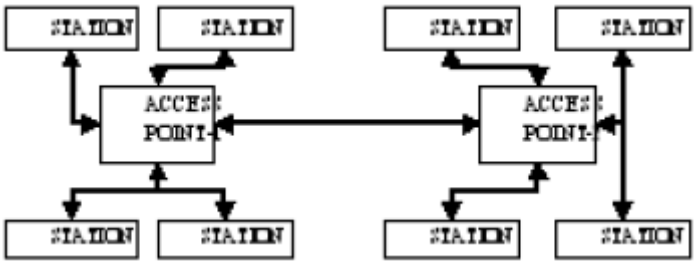

Figure 3.4(4): AP Based WLAN Location Detection Architecture

3.5 Selection of WLAN Location Detection Architecture

After detailed study of the location detection architectures and WLAN location detection architecture described above we have selected the **Client-Server Based WLAN Location Detection Architecture** taking advantage of its **Offline Phase.**

Reason of selecting this architecture is first of all its easy to implement and we have many deployed scenarios of this architecture especially in our work environment, so that we can have many feedbacks which can help in resolving the complications of this architecture during its deployment. As much as we will be clear about the KPIs regarding the deployment of this architecture we will have more accurate results at the end.

3.6 Summary

This chapter includes the detailed study of the methods or techniques that helps in WLAN location detection and also the threats in relevance to the location detection or the Location Based Services that uses the location information of users. Further we have described in detail the kind of architectures used by LBS based applications. Finally the selection of WLAN location detection architecture for this research with reason of its selection.

Chapter 4

Developed Architecture and Proposed Technique For WLAN Location Privacy

4.1. Introduction

This chapter presents our proposed technique for the WLAN location privacy. We have tried to describe different sections and outlined goals in this Chapter to provide the clear understanding of the proposed technique. As mentioned earlier there several researches and work done to prevent the user WLAN location information which are described below.

4.2. Related Work

There are several researches have been done in order to prevent the sharing of wireless user location information from being used for any offense. Location privacy wouldn't be concern if there are no such demands of services and applications that uses the location information of the users, in order to prevent this one technique that has been developed and adopted is through the obfuscation of the user location information which randomly alters the location information of the user received though the sensing devices [11]. Another useful technique is landscape aware location privacy protection which is an advanced technique that builds on the fundamentals of obfuscation technique that is initiated by a trusted agent and consists of artificial perturbation of location information by sensing devices. This technique provides the map dependent obfuscation which releases several users' location information that guarantees that the provided information never violates the original user location information to the requester not even after refining through map based inference [8]. Leading towards another proposed technique to prevent user location information, is the provision of several false user location information with actual user information in response to the LBS requests from service provider, as the service provider cannot differentiate the actual user location the user's location information is protected [9].

The one very interesting location privacy technique in the WLAN domain is obfuscating the location information request initiator by changing / updating the interface identifiers and by DMAS [12] so that an adversary cannot track an individual user on long term movements. One good technique is vagueness based obfuscation [10] for protecting location privacy which shares the Parent location information instead of sharing the actual location for example if user is in one of the street then it shares the block information with the requestor and as one block has several streets so the adversary cannot guesses the actual location of the user.

4.3. Design Goals

In order to develop the WLAN location privacy technique we need to develop a model in such a way that it fulfills the prerequisites of Server Client based location detection architecture, to achieve the above mentioned conditions we have carefully identified the design goals which are mentioned below:

- **Adequate selection of Wireless AP and IOS –** In order to develop WLAN location detection architecture selection of wireless AP is one of the major components. Selected AP should be capable of covering larger area of each location so that every client should have reliable connectivity. AP should only listen to their controller which means that AP should be selected in a way that they can be converted to Lightweight AP from Autonomous AP. These are the two types of wireless AP, Autonomous AP has the capability to make decisions on its own and is the only master if itself where the Lightweight AP is like salves and makes decisions as commanded by their master (WLAN Controller). We have selected the Cisco Aironet 1140 APs in our architecture and to convert the AP from Autonomous to Lightweight AP we have taken Lightweight AP IOS which was loaded in to each of the AP so that they can be controlled via central appliance. In our architecture converting an AP into Lightweight is mandatory it has advantage from security point of view too because no one can control or have access to the Lightweight AP even if it is connected via that AP where Autonomous AP can be accessed and can be compromised remotely by generating several attacks.

Figure 4.3(1): Cisco Aironet 1140 AP

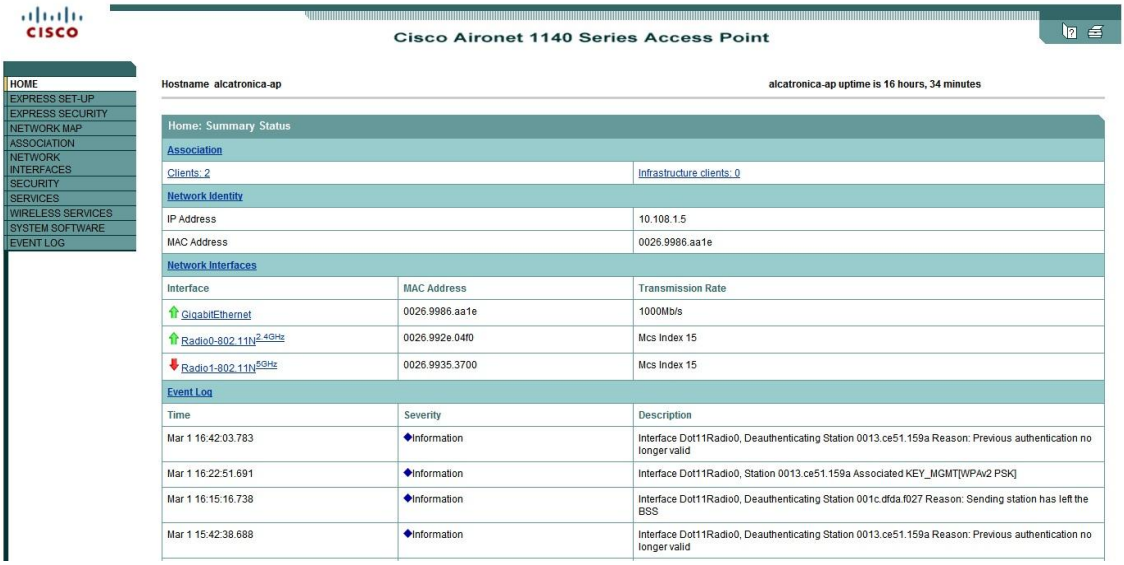

Figure 4.3(2): Cisco Aironet 1140 AP GUI Console

- **Selection of supported WLAN Controller -** After the selection of AP with their conversion to lightweight AP (salves) we need a suitable WLAN controller (master) that should be capable of managing total number of APs in WLAN we need to setup an environment where we can have the details of all the clients at one place and also we can easily manage all AP from one central location for this we have selected the Cisco 5508 WLC.

Figure 4.3(3): Cisco WLAN Controller

- **Installation and configuration of WLC -** WLAN controller should be configured such that it can search all the lightweight AP and can register them

in its database, for this Cisco WLAN controller and all AP should be in the same network or if on different network then they must be reachable from WLC.

- **Configuration of Aggregation Switch –** In order to provide communication to WLC and the lightweight AP there must be an aggregation switch that physically connects each of the AP and the WLC with it. Switch must have all ports be secured configured and should have DHCP server configuration so that anyone who physically connects to it should be assigned with a schematic IP address. All the LWAP assigned with DHCP IP should be configured for Static DHCP so that they always get the same IP Address after reboot.
- **Registration of All AP with WLC -** All the AP should be loaded with LWAP IOS, LWAP when power on requires IP to be assigned from DHCP server, all the LWAP should be assigned with schematic IP Address of the same network so that they can provide communication all the clients connected to them with each other regardless of the parent LWAP locations. All the LWAPs should reachable to the WLC. As soon as all the LWAPs gets their IP address assigned they initiates the LWAPP query request for their controller which are when received by controller responded and LWAP get registered them with the WLC.
- **Configuration of WLAN Security Parameters –** Keeping all client server communication secure within the WLAN it is necessary to configure some security parameters, as enhanced as the security parameter will be, more secured communication will be between the server and clients. To achieve the security communication and secure entities within the WLAN the communication channel should be secured with WPA/WPA2 with AES-256bit encryption and there should be wireless MAC Filtering or any suitable authentication method for clients registration in the WLAN (i.e. LDAP / 802.1x should be configured) so that no client server communication can neither be hijacked nor a masquerader can step in.
- **Configuration of WLC Access for Server to WLC Communication –** In order to collect the client's signal and association information w.r.t. each LWAP on a standalone server, WLC should be configured to provide that database server a secured access.

- **Configuration of Standalone Database Server –** There must be a standalone machine which acts as a server and storing the useful cliental information which is used for our intended purpose of preventing location information of the WLAN users from being shared with any adversary or for any offensive act.
- **Middleware application between untrusted user and database server –** There should be a middleware application designed in a way that takes the user input to find location of the desired WLAN user and reverts the results as per defined policy or critical user list.

4.4. Proposed Technique

As mentioned above that we have taken advantage of the Client Server Based Architecture of WLAN Location detection in order to derive the technique of WLAN Location Privacy. We have subdivided this section to elaborate the deployment details at each step so as to provide the clear understanding of the proposed technique. This technique has the fundamentals of Cisco WLAN controller based deployment model which is now adopted by most of the corporate sectors of the market due its ease of deployment and management of hundreds of wireless users over the entire corporate environment. Other then corporate environments it is also considered to be deployed in financial, educational, medical institutions and in hotels, resorts, motels and public places as well. We have started working on our technique with the deployment of this model and then based upon this model we have taken advantages of its friendly environment and detailed cliental signal and association information. Moving towards the detail description of our technique we would like to inject your attention on the below defined subsections which will take you deep into the roadmap of this technique.

4.4.1. Upgrading Autonomous AP to LWAP and Their Installation

Starting with the architecture development, the necessary component is configuring the Cisco wireless AP so that they can placed in available region in a way that their signals space covers maximum possible place of the selected area with no signal space overlapping. Cisco AP comes up with autonomous AP IOS version and in order to make them to listen to one controller there should be LWAP IOS loaded on each of the AP in the whole area. All the autonomous AP will be upgraded to LWAP

using the respective IOS and loaded it on each of the autonomous AP [13]. After upgrading the APs they are mounted on each of the predefined locations (by conducting the wireless survey [14]) in order to cover the complete area with the signal space of each LWAPs. Each LWAPP is connected with UTP cable which is reaching at one central location where an aggregation switch will be placed in order to connect them all on one network.

4.4.2. Formation of Radio Map

The second most important step is the construction of Radio Map that represents the complete physical layout of the whole campus with each department mentioned separately. After this we added the positions of LWAP in each department and constructed a table of approximate distances against the RSSI values which will help in identifying the approximate location of the WLAN user by comparing the RSSI values and the associated LWAP location in campus. Below are the observed values of RSSI at different distances from each LWAP.

Distance From LWAP (meters)	WLAN User's RSSI (dB)
1-5	-20 ≈ -25
5-10	-25 ≈ -35
11-20	-35 ≈ -40
20-30	-40 ≈ -45
30-40	-45 ≈ -50
50-60	-50 ≈ -55
60-70	-55 ≈ -60
70-100	-60 ≈ -75
100-150	-75 ≈ -93

Table 2: Estimated Values of RSSI against Distances

4.4.3. Configuration of Aggregation Switch

Aggregation switch will be responsible of connecting the wireless clients, LWAPs and WLC to one network. In our technique we have configured switch for port security and as DHCP server so that it can assign the schematic IP addresses to

the wireless clients and LWAPs (only in initial discovery phase). All the LWAPs and WLC are then physically connected to aggregation switch via UTP cables.

4.4.4. Configuration of Cisco WLAN Controller

Configuring Cisco WLC includes the below mentioned steps:

Configuration to connect with Aggregation Switch – WLC we configured consists of 8 physical interfaces in which we have configured one of the physical interfaces as its management interface and other as trunk port that is for carrying the traffic from all the wireless clients.

Registration of Cisco LWAPs – Whenever the LWAP reloads itself or refreshes its services it broadcasts the search query to find its WLC using LWAPP or CAPWAPP this is the protocol that can be only understandable to the LWAP and WLC. WLC responds the LWAP with it identity telling them about its position as Controller in the WLAN. LWAPs then store the replied information in their NVRAM and always contact their controller for decision making. After registration of all the LWAPs they are named with respect to their placement (i.e. name of departments, sub-departments or others) so that they can be easily identified.

Configuration of Security Parameters on WLC – To prevent the WLAN user communication and the complete WLAN from unauthorized users below mentioned security parameters have been configured:

MAC Filtering – In order to prevent the un-authorized user / masquerader from being a part our WLAN we have configured the WLAN users MAC filtering by entering the only valid WiFi MAC addresses of users in WLC MAC Filtering list.

WLAN Communication Security – In order to prevent the client server communication WLC is configured with WPA/WPA2 with AES 256-bit encryption so that no adversary can impersonate and the WLAN and compromise the server that stores the location information of the WLAN users.

WLC Access Configuration for Database Server – To achieve the goal of WLAN location privacy the database server must communicate securely with Cisco WLC so that it can store the location information of all the connected WLAN users for the application of privacy technique and no unauthorized users can have the access to WLC.

4.4.5. Configuration of Database Server

The main component of our proposed technique is the database server that is used to store the signal and association information of the connected WLAN users. We have installed Microsoft Server 2008 R2edition on it, the minimum specs of the system required for database server is mentioned below:

Requirement	Standard Edition	Enterprise Edition	Datacenter Edition	Web Edition
Minimum CPU Speed	133 MHz	133 MHz for x86-based computers 733 MHz for Itanium-based computers*	400 MHz for x86-based computers 733 MHz for Itanium-based computers*	133 MHz
Recommended CPU Speed	550 MHz	733 MHz	733 MHz	550 MHz
Minimum RAM	128 MB	128 MB	512 MB	128 MB
Recommended Minimum RAM	256 MB	256 MB	1 GB	256 MB
Maximum RAM	4 GB	32 GB for x86-based computers 512 GB for Itanium-based computers*	64 GB for x86-based computers 512 GB for Itanium-based computers*	2 GB
Multiprocessor Support **	Up to 4	Up to 8	Minimum 8 required Maximum 64	Up to 2
Disk Space for Setup	1.5 GB	1.5 GB for x86-based computers 2.0 GB for Itanium-based computers*	1.5 GB for x86-based computers 2.0 GB for Itanium-based computers*	1.5 GB

Table 3: Minimum System Requirement for Win Server 2008 R2

The database server is configured to access the WLC on periodic time interval and to collect WLAN users' complete information via designed windows scripting, the collected information mainly includes its MAC, RSSI value and assigned name of the LWAP with which it was associated at the time when the information collected. This information is exported to a simple excel file with the timestamp at which the configuration was taken from Cisco WLC. This information is used by the designed application to search the location definition attributes after the input of the untrusted user.

4.4.6. Middleware Application Development

This is the component which is the actual front end for the untrusted user who is requesting to find current / last location of any of the WLAN user. This application resides on the database server and is accessible from its web console within the WLAN. Reason for making this application accessible from WLAN is that we have tried to develop it in a way that it can help in detecting the location of the WLAN user except the critical users who have granted permission for location prevention (i.e. users who have valid reasons to hide their location information), this case is valid in an environment where we need to keep users under monitoring for example WLAN users in a University or Military Campus. In case where we need to hide the location information of all the WLAN Users (i.e. public places) we can set a policy that is permitting all users to obfuscate their location information.

4.5. Summary

In this chapter we have pointed out and described each of the segments with its functionalities and the reason of their selection. Each segment has its own value in the implementation of the complete technique and hence discussed in detail separately. In conjunction with this we have also referred the technique of radio map formation and construction of distance measuring table using RSSI values. In the end of this chapter we have also included the fundamentals of the front end application and server machine.

5. Application of Proposed Technique on Client Server Based WLAN Location Detection Architecture

5.1. Introduction

This Chapter will present a detailed implementation of our proposed technique and its implementation on Client Server Based WLAN Location Detection Architecture.

5.2. Architecture

Our architecture consists of above 50 clients with WiFi equipped devices that are compliant to IEEE802.11a/b/g standards and are spread across the entire campus. To provide uninterrupted WLAN connectivity to each of the user we have placed 10 Cisco Aironet 1140 AP after conducting a successful indoor WLAN site survey which ensures that none of the area within the boundaries of our institute left uncovered with wireless APs signal space. We have selected a suitable place as a central position where we can easily setup for the installation of aggregation switch and WLC also from where we can easily provide the physical connectivity from aggregation switch to all of the LWAPs located at different places. After this setup all the LWAPs are connected to the ports of aggregation switch. Our aggregation has the POE functionality so that we don't have a need of any other power source for LWAPs.

On successful connection of all the LWAPs with the aggregation switch we proceeded with connecting Cisco WLC5508 with the aggregation switch so that we can have all the AP (Slaves) and WLC (Master) within the same Layer2 (MAC Layer) boundaries. Controller based WLAN environment has the biggest advantage of providing secured WLAN infrastructure with ease of management of even 500 WLAN users and due to this reason we have selected this architecture. After complete setup of this controller based environment we have integrated a standalone machine fulfilling the minimum requirement as mentioned in the Table 3, and installed windows Server 2008 R2enterprise edition on it, selecting the server edition is also one of the reason to provide secure infrastructure and as it will be a server that is

storing the complete WLAN clients signal and association information so it should be configured with secured parameters. This server will be the backend appliance that is acting as a central location information provider / preventer to / from untrusted user's queries.

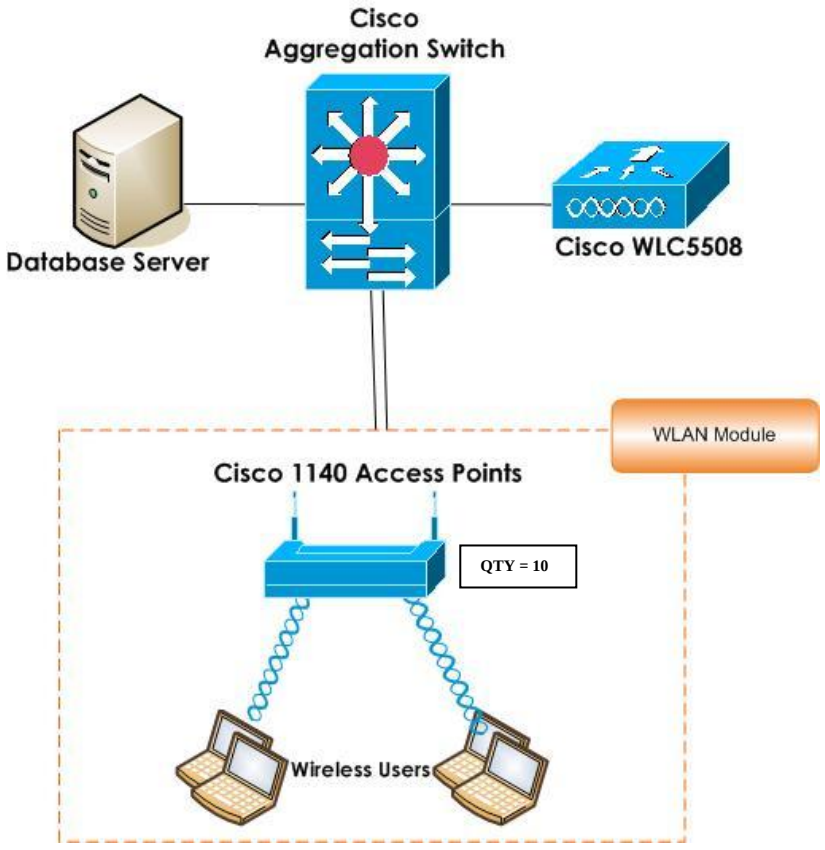

Figure 5.2(1): Deployed Client Server Based WLAN Location Detection Architecture

Below are the brief details of the application with illustrations of implementation at each of the phase of deployment of proposed technique.

5.3. Description to Implementation Phases in WLAN Location Privacy Technique

We have elaborated the upshots of the application of our proposed technique on the WLAN Client Server Based Architecture in the below sub-sections;

5.3.1. Configuration of Aggregation switch for DHCP Server

In order to configure the aggregation switch we have first configured it for providing secured access after which we have designed an IP Schema through which we can organize the assignment of the IP addresses of the WLAN clients and LWAPs.

Below illustration depicts the configuration done to make aggregation switch a DHCP Server.

```
!
ip dhcp pool INSIDE_LAN
   network 192.168.204.0 255.255.254.0
   default-router 192.168.204.1
   dns-server 192.168.202.55 192.168.202.56
   lease 0 10
!
```

Figure 5.3.1: DHCP Configuration CLI Commands on Aggregation Switch

5.3.2. Configuration of Cisco WLC

In order to configure let the LWAP registered with the WLC, allow communication between each of the WLAN clients and between client and server though client is connected via any of the LWAP we need to configure WLC. Also we need to configure the access of WLC for server and administrative use. Keeping security a mandatory part of this architecture we also configured the security parameters defined above in order to prevent the impersonation during the client server communication and also to avoid unauthorized participation of the client. Below illustrations will depict the results of the configurations done on Cisco WLC.

Figure 5.3.2(1): WLC Interface Configuration for Connectivity with Agg. Switch

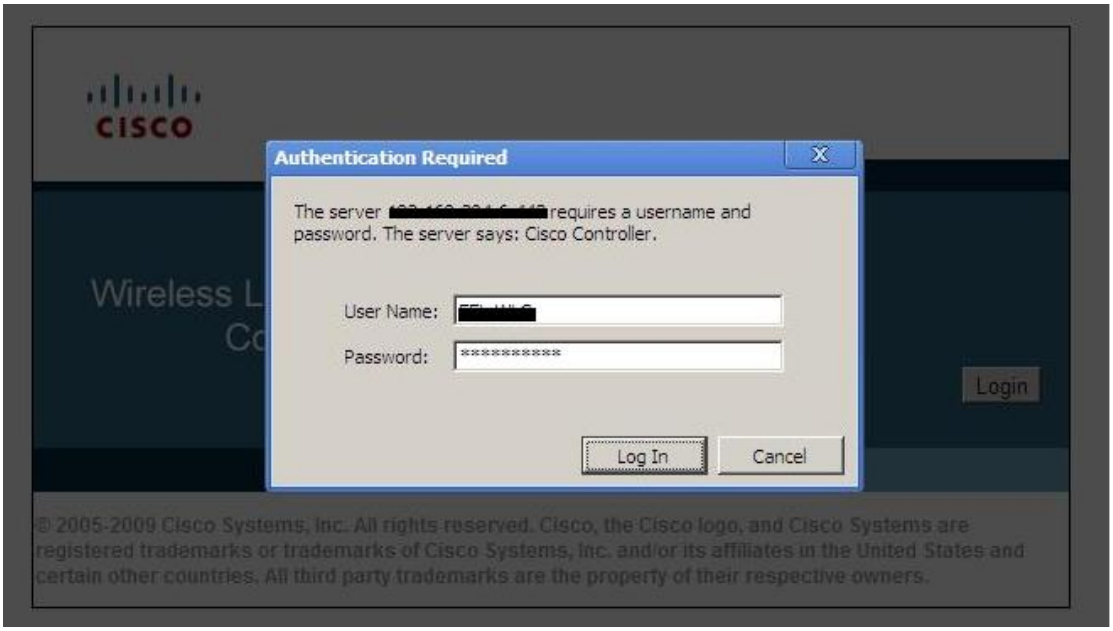

Figure 5.3.2(2): WLC Access Control Configuration

Figure 5.3.2(3-a): WLC Configuration for WLAN Communication Security

Figure 5.3.2(3-b): WLC Configuration for WLAN Communication Security

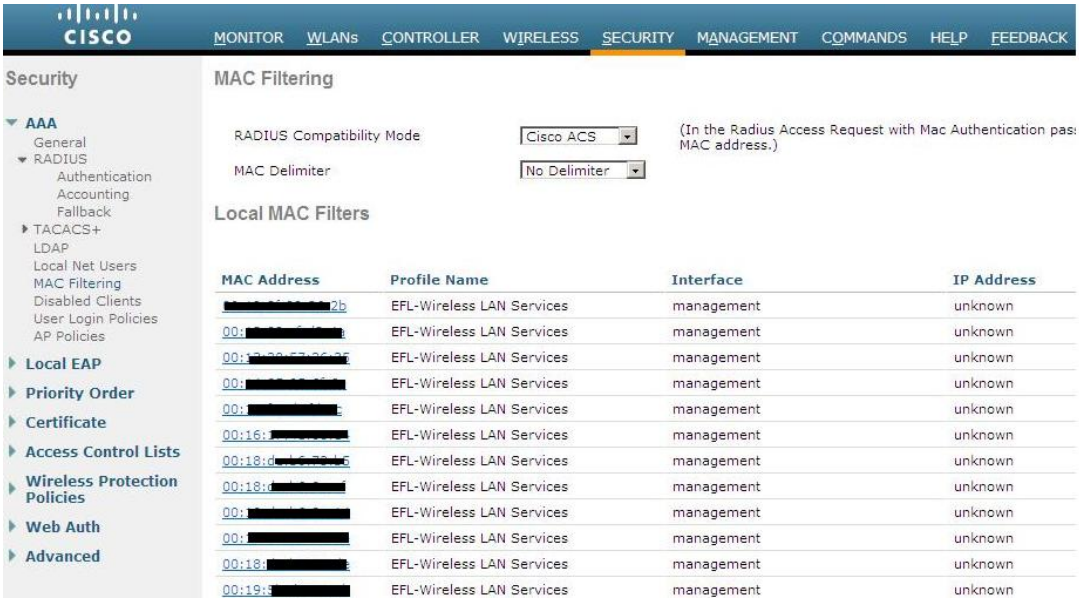

Figure 5.3.2(5): WLC MAC Filtering for Un-authorized Access Prevention to WLAN

5.3.3. Autonomous to LWAP Upgradation

As soon as we plugged in the UTP cable in to the Ethernet port of the AP it detects POE and turns itself to on and initiates DHCP query to the DHCP server which is responded by the aggregation switch acting as a DHCP server. AP is assigned with the IP from the DHCP pool and is then accessed via web console for the

upgrade. Below illustration shows the step we performed to upgrade the autonomous AP to LWAP.

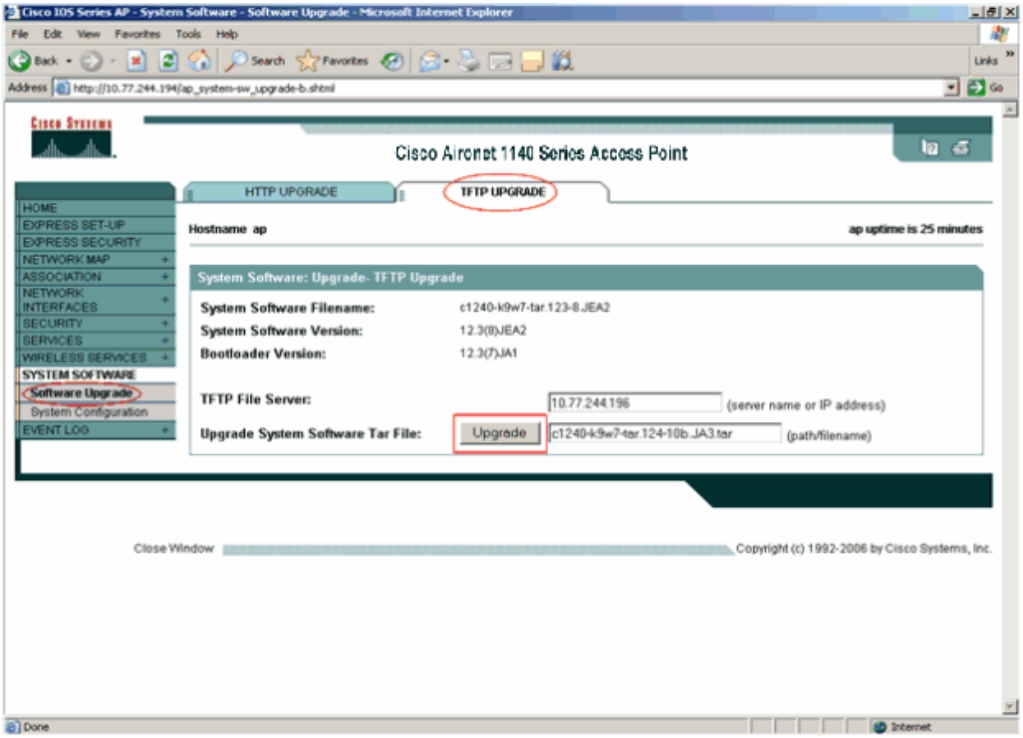

Figure 5.3.3: Autonomous to LWAP upgradation

5.3.4. Registration of LWAPs on WLC

As soon as we upgrade the APs to LWAP and reboots they after reboot broadcasts the LWAPP controller (master) search which is responded by WLC and LWAP stored the information of their server in their memory and always ask their controller for decisions. Below is the snapshot illustrating the registration of LWAP on WLC.

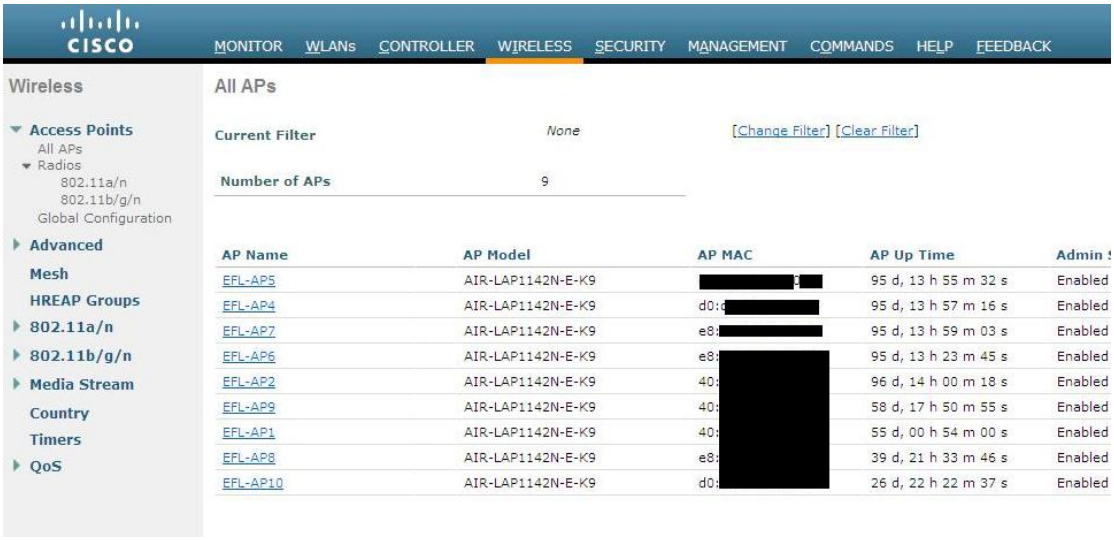

Figure 5.3.4: WLC LWAP Registrations

5.3.5. Verified WLAN Client Connection Profile and Received Information

After complete setup of Controller based WLAN environment we have verified the connectivity of the client with the security parameters configured and also observed the cliental signal and association information at Cisco WLC. Below are the snapshots which are self explaining the verification of the configurations.

Figure 5.3.5(1a): WLAN Client Detailed Information at WLC

Figure 5.3.5(1b): WLAN Client Detailed Information at WLC

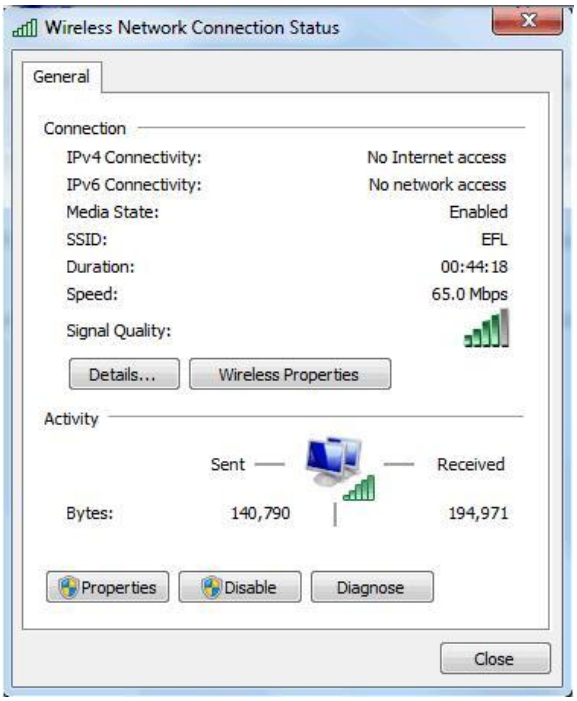

Figure 5.3.5(2a): WLAN Client End Information

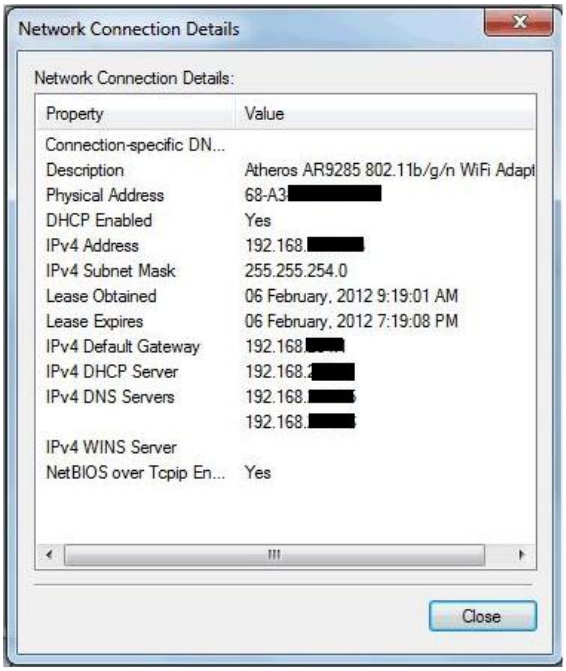

Figure 5.3.5(2b): WLAN DHCP IP Settings

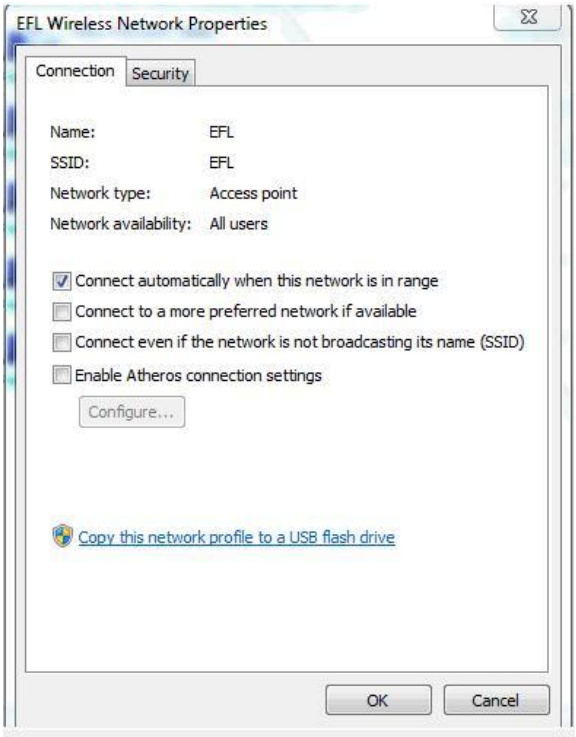

Figure 5.3.5(2c): WLAN Security Settings

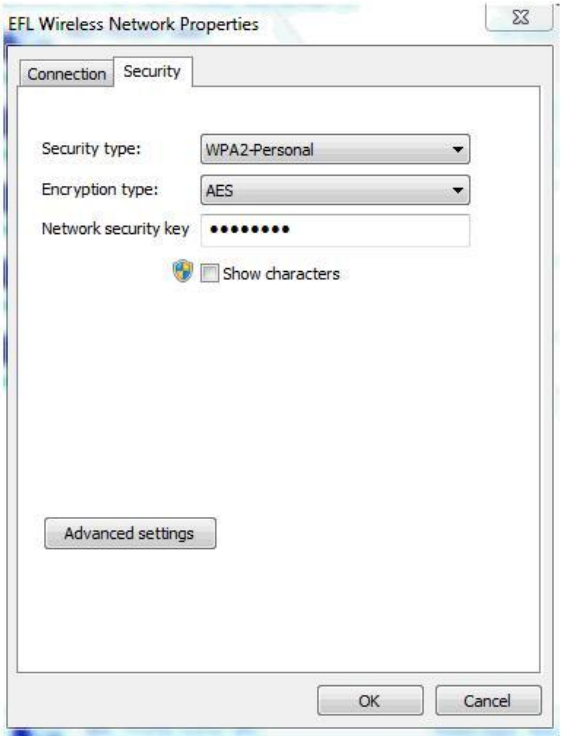

Figure 5.3.5(2d): WLAN Security Settings

5.3.6. Database Server Configuration

As per above illustrations in which we have seen the cliental details of its signal and association information we can now setup the database server that has the responsibility of collecting information of each of the WLAN client from WLC and stores it in a central database which will then accessed by the middleware application. To achieve this we have followed the below mentioned major steps:

Configured Secured Access to WLC – In Cisco WLC we have configured a username which is less privileged and can only run ‘show’ commands.

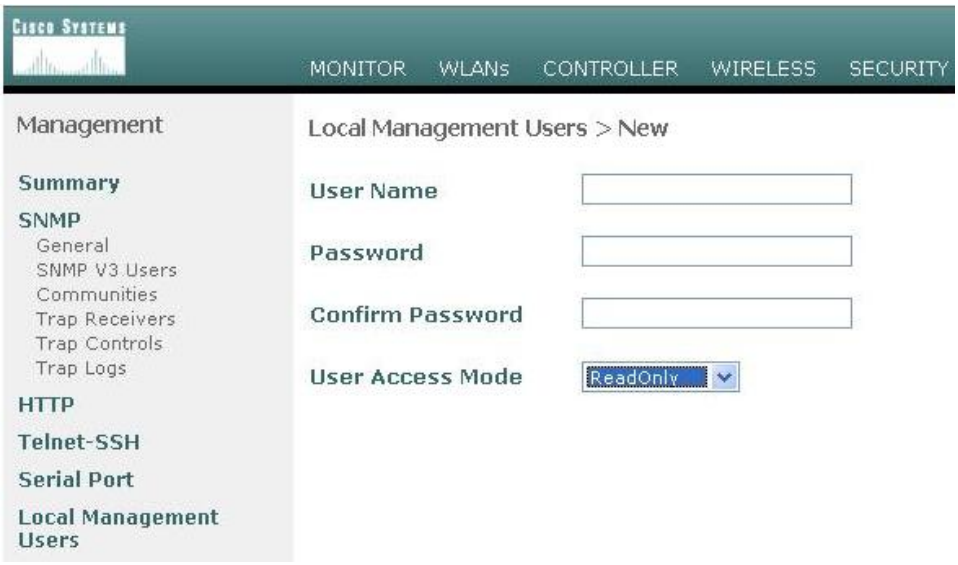

Figure 5.3.6: WLC Read-Only User Account for Database Server Access

Whenever the server initiates request to Cisco WLC for WLAN Clients information it always uses the configured account with fewer privileges so that even if the server gets compromised it cannot provide ways to perform configuration changes in WLC.

Writing Windows and VB Script for Information Collection – To access the Cisco WLC we have written windows based script which will access the Cisco WLC, executes commands on Cisco WLC and will then stores the information in a file which will be referred by the middleware application during making decision of what and only when true information will be shared with the untrusted user. Sample scripts are illustrated below:

VB Script	Set cloner = CreateObject("WScript.Shell") cloner.run"cmd" WScript.Sleep 500 cloner.SendKeys"telnet 192.168.x.x -f C:/**WLAN-Client.xls**" cloner.SendKeys("{Enter}") WScript.Sleep 500 cloner.SendKeys"admin" cloner.SendKeys("{Enter}") WScript.Sleep 500

	cloner.SendKeys"admin123" cloner.SendKeys("{Enter}") WScript.Sleep 500 cloner.SendKeys"show client ccx rm report beacon" cloner.SendKeys("{Enter}") WScript.Sleep 500 cloner.SendKeys"qquit" cloner.SendKeys("{Enter}")
Windows Script	wscript myscript.vbs

Table 4: Windows and VB Script for WLC Access and Information Collection

The output from the script will be stored in a file:

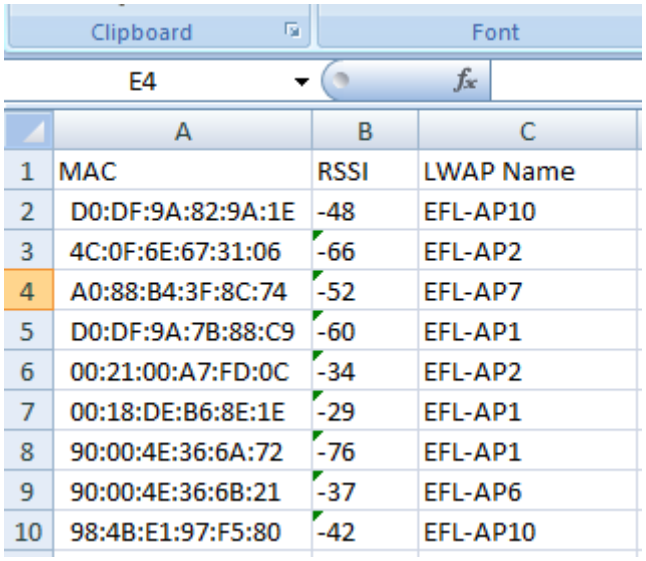

Table 5: Output File from Written Scripts Carrying WLAN Client Information

5.3.7. Middleware Application Design

To provide the front end user input environment where he can enter the MAC of the user whose location he want to know. Application different modules and functions in it which can prevent the critical user location information (enlisted as per defined protection policy) and also shares the location information of normal user (user's not included in the list defined by protection policy). The protection policy

that states which of the user will be prevented (obfuscated location information will be provide against that user) and which are not can be changed according to the business or environmental need. Below is the flowchart of the designed middleware application which interacts with the database server for providing WLAN location Privacy and also location detection.

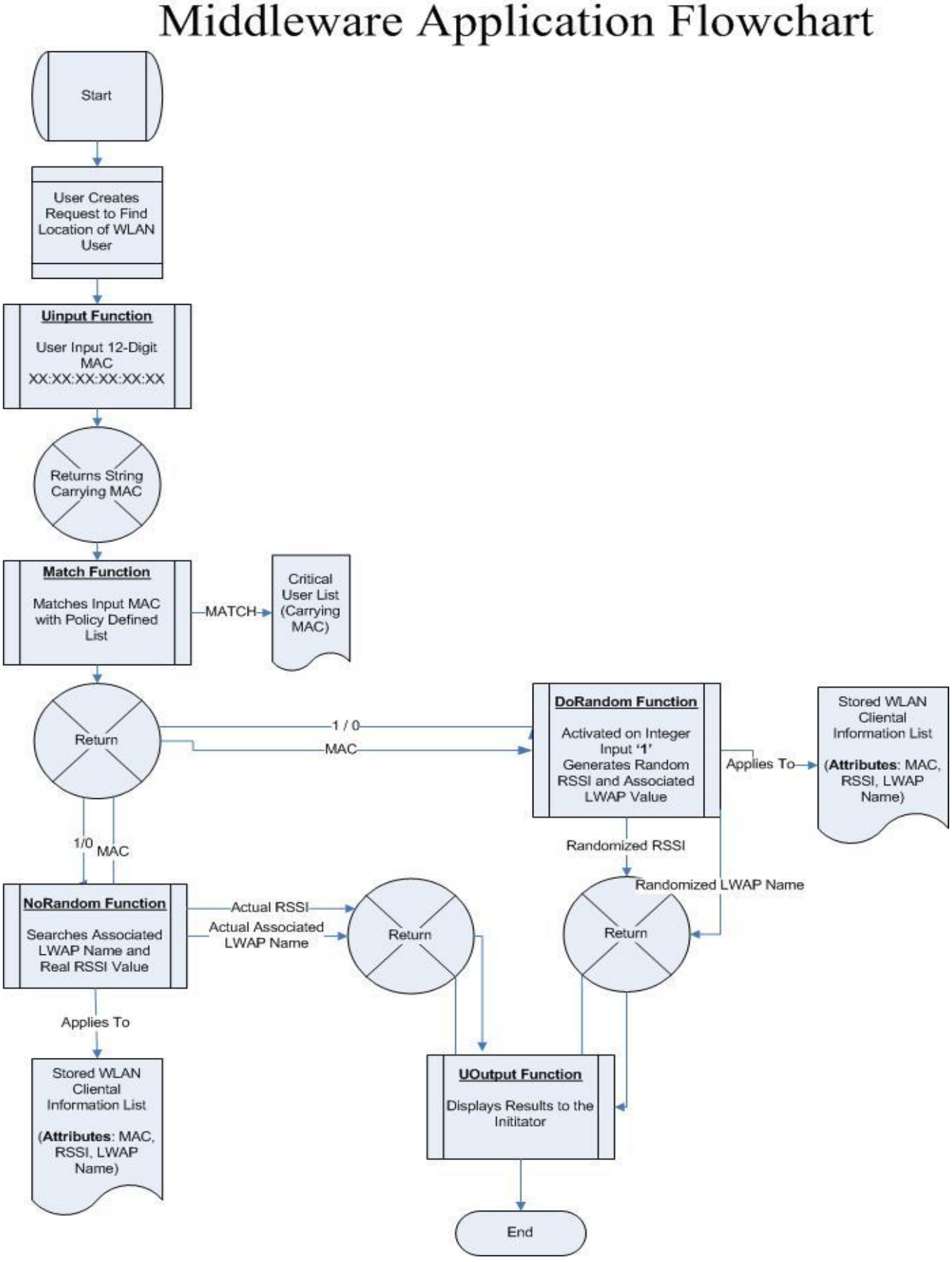

Figure 5.3.7: Middleware Application Flowchart

Description of Functional Flow of Application

‘UInput’ Function– Application has a function that takes a user input of 12-digit hexadecimal value with ‘:’ after every two digits (i.e. 00:AF:EF:TY:WE:3D), the input will actually be a MAC address of the WLAN user to which untrusted user want to locate.

‘Match’ Function – Match function will first refer the list which is defined with the user’s identity as per policy which permits the critical user only whose location needs to be prevented. This functions returns Integer ‘**1**’ and a string of hexadecimal input value from ‘**UInput**’ on success which means the MAC entered is of the user which is permitted in the policy and its location need to be prevented, and returns Integer ‘**0**’ and a string of hexadecimal input value from ‘**UInput**’ in case of no match.

‘DoRandom’ Function – This functions received the values from ‘**Match**’ and only activates on integer input ‘**1**’. This function refers the database sheet of WLAN users’ collected information and applies random function on the two different fields individually ‘**LWAP Name**’ (comprises of configured names of all LWAPs) and ‘**RSSI**’ (comprises of all active WLAN user’s RSSI values). The function returns the randomly collected information (string value and –ve integer value) from ‘**LWAP Name**’ field and ‘**RSSI**’ field.

‘NoRandom’ Function – This function too receives values from ‘**Match**’ function and only activates on ‘**0**’ input. It simply refers the database sheet of WLAN users’ collected information and matches the ‘**MAC** field with the input string and returns the respective values (string value and –ve integer Value) in ‘**LWAP Name**’ field and ‘**RSSI**’ field.

‘UOutput’ Function – This function take inputs (String and –ve Integer) from ‘**DoRandom**’ or ‘**NoRandom**’ and displays as an resultant output to the request initiator.

Above defined were the major functions used to develop a middleware application which is providing a frontend to the user queries and their outcomes, the received values will then be compared with the constructed Radio Map (section 5.4.2) to find the user’s location information.

5.3.8. Illustration of Developed Application

On the basis of previously defined flowchart and the algorithm we have developed an application to formulate the output and observe its behavior on different inputs which will be then compared with selected technique [12]. Below are the illustrations of the cases when:

- **CASE1:** User Input MAC address of a Non-Critical User in WLAN / WCAN for whom we do not need to prevent location information.
- **CASE2:** User Input the MAC Address of a Critical User (as defined in the list ‘**critical mac**’ list) in WLAN / WCAN whose location information needs to be prevented.

Defining critical / non-critical user will always depends on the scenario / environment of consideration as it is not necessary that, having location information of a user which is critical in one scenario will always be critical in another scenario. For example in a Campus we do not need to prevent location information of each of the student studying there infact we will be curious about their location information in campus so that they can be monitored for their presence, however in a Campus we need to prevent the location information Campus Dean and designated faculty members so that no one can trace their location information to make them a victim for their criminal activities. In both the cases application will refer the below two information to view the results as per their defined logics.

MAC	RSSI	LWAP Name
D0:DF:9A:82:9A:1E	-48	EFL-AP10
4C:0F:6E:67:31:06	-66	EFL-AP2
A0:88:B4:3F:8C:74	-52	EFL-AP7
D0:DF:9A:7B:88:C9	-60	EFL-AP1
00:21:00:A7:FD:0C	-34	EFL-AP2
00:18:DE:B6:8E:1E	-29	EFL-AP1
90:00:4E:36:6A:72	-76	EFL-AP1
90:00:4E:36:6B:21	-37	EFL-AP6
98:4B:E1:97:F5:80	-42	EFL-AP10

Table 5: Output File from Written Scripts Carrying WLAN Client Information

F22 f_x

	A	B	C
1	MAC	RSSI	LWAP Name
2	D0:DF:9A:82:9A:1E	-48	EFL-AP10
3	98:4B:E1:97:F5:80	-42	EFL-AP10
4			

Table 6: Critical User List Exists As A Part Of WLAN

CASE 1 – In this case user will input the MAC Address of a non critical user and the application will display the actual user location information. Below are the illustration of the user inputs and the application output as per defined conditions in it.

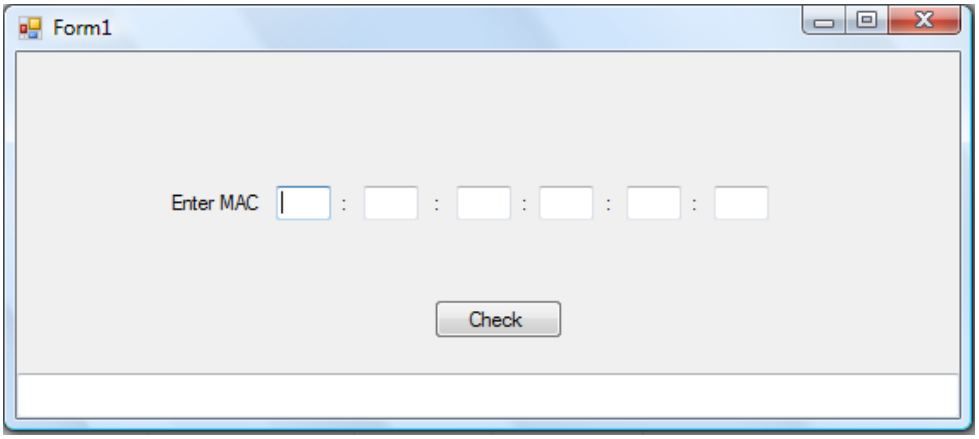

Figure 5.3.8(1): Application User Input Window

As an example we are taking user with MAC: A0:88:B4:3F:8C:74 which is a non critical user and is not defined explicitly in the '**critical mac**' list (Table 6).

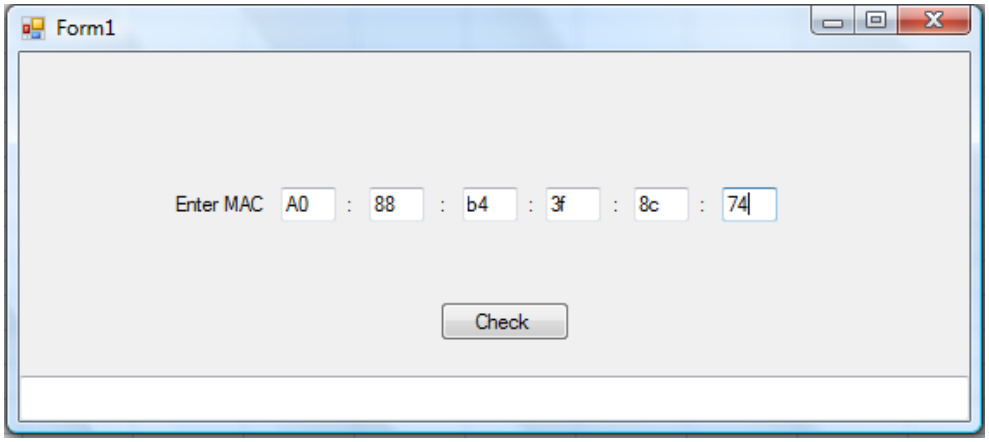

Figure 5.3.8(2): Non-Critical User's MAC Input in Application

After Entering MAC address of the non critical user application will display the actual association request.

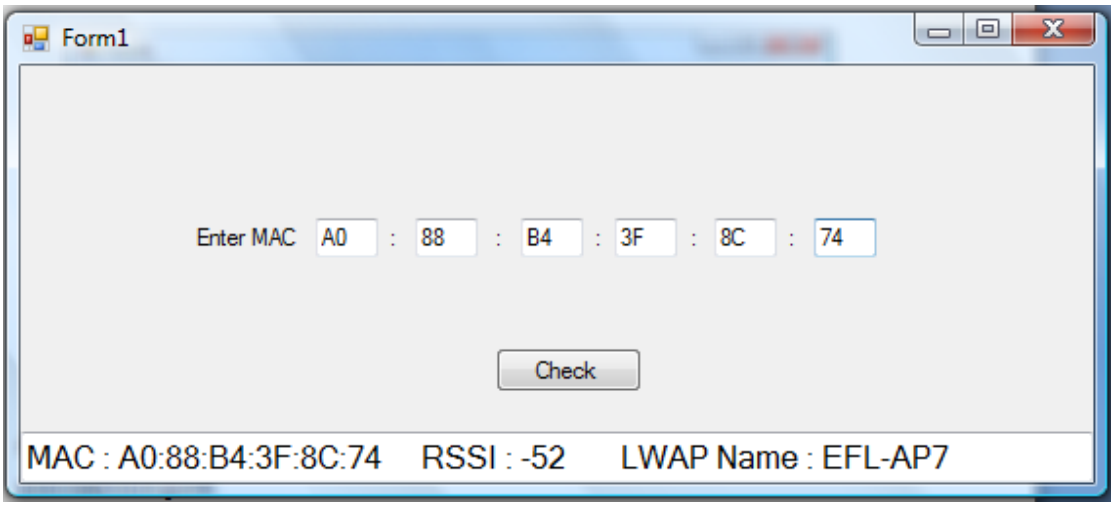

Figure 5.3.8(3): Application User Location Information Output

If we compare the application output information with the actual list carrying the information of the all the WLAN clients you can conclude the correctness of the results.

CASE 2 – In this case user will input the MAC Address of a critical user (as defined in the Table 6) and the application will display the false user location information which will always be a random one but will seems like a legitimate

information as it will show requester a value in between current available LWAPs and also in between the reasonable but random RSSI value which will protect sharing of critical user location information. Below are the illustration of the user inputs and the application output as per defined conditions in it.

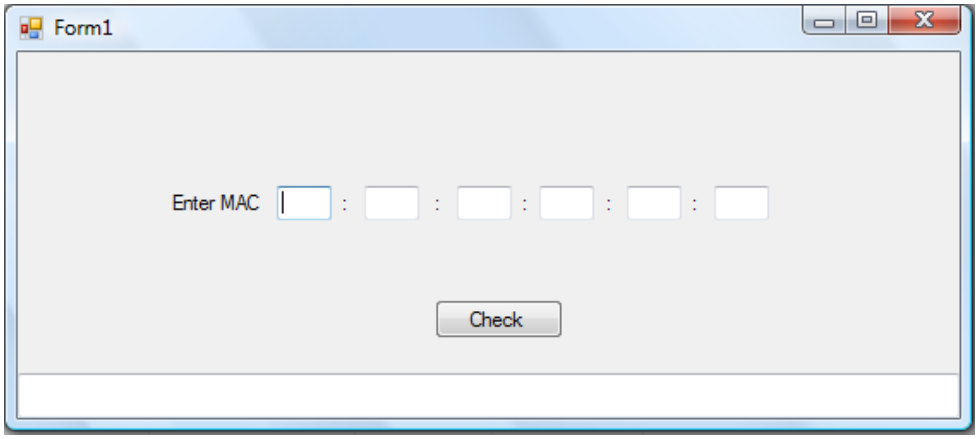

Figure 5.3.8(1): Application User Input Window

As an example we are taking user with MAC: D0:DF:9A:82:9A:1E which is a critical user and is defined explicitly in the '**critical mac**' list (Table 6).

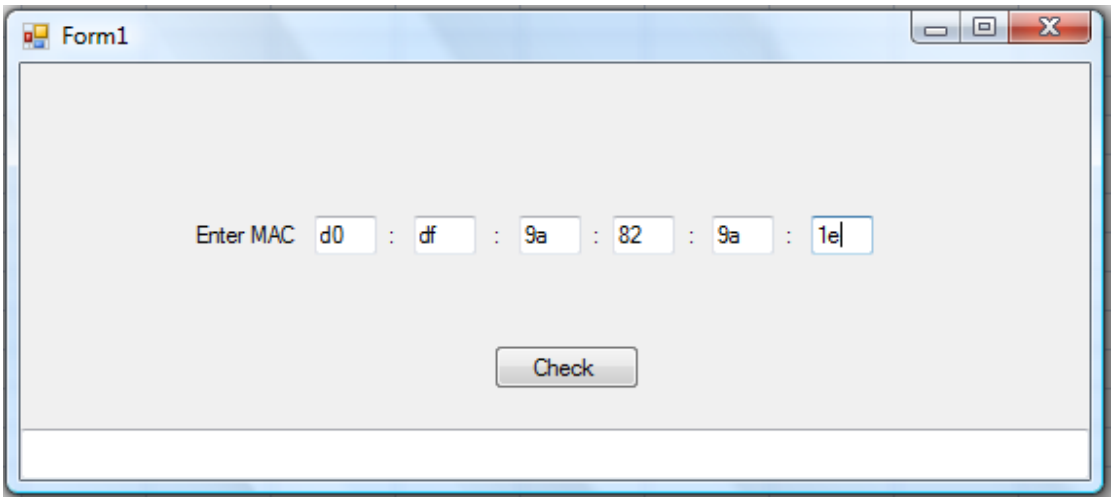

Figure 5.3.8(3): Critical User's MAC Input in Application

After Entering MAC address of the critical user, application will display the random false location information data.

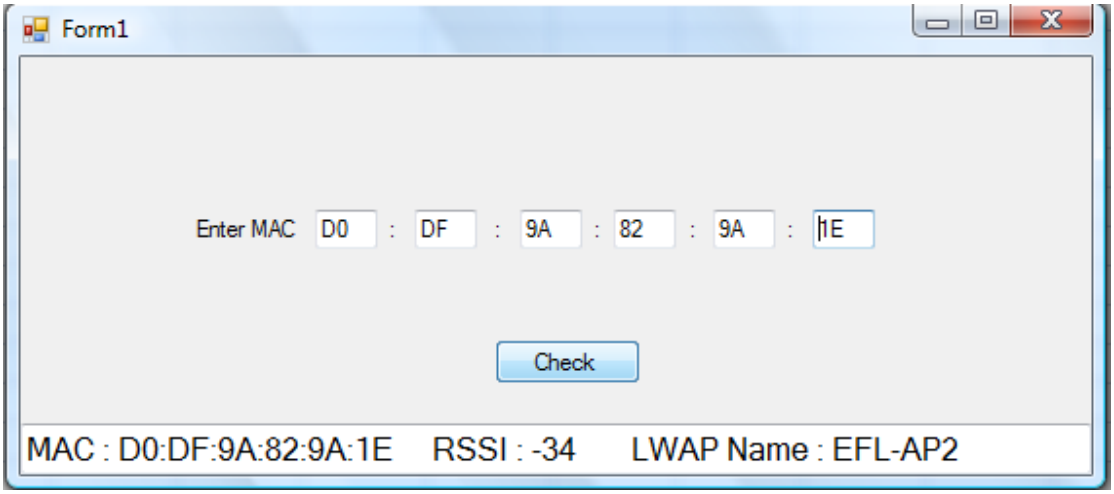

Figure 5.3.8(4): Application User Random Location Information Output

If we compare the application output information with the '**critical mac**' list (Table 6) carrying the information of critical WLAN clients you can conclude the incorrectness of the results. Lets again check for the same MAC Address.

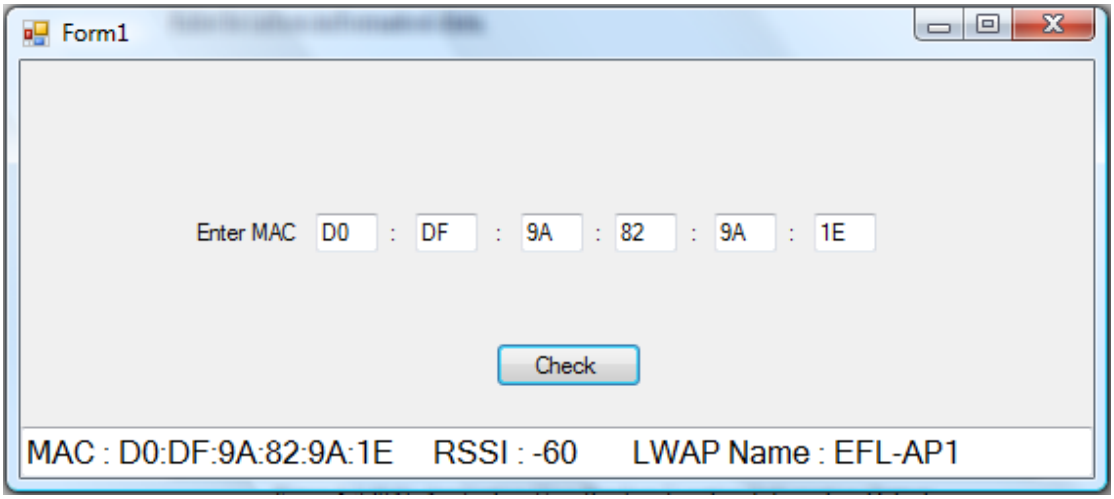

Figure 5.3.8(5): Application User Random Location Information Output

5.4. Summary

This chapter is the core segment of the research which includes the complete implementation of the proposed technique. Starting from the collection of resources, planning for its implementation we have ended up with the final outcome of our research with illustration of the results in each segment of implementation phase. It describes all the steps we have followed from the surveying, implementation of WAP, installation of core switch, upgradation of WAPs to LWAPs, their registration with controller, server secured communication and collection of attributes used for user's location detection, running of scripts on server to store the information and finally the complete framework of middleware application and its behavior on different input has been observed.

6. Analysis of Proposed Technique

6.1. Introduction

This chapter presents a brief analysis of our proposed technique with respect to the design goals. Comparison of proposed technique with the obfuscation technique by DMAS [12].

6.2. Analysis

The analysis of our proposed technique with respect to the predefined design goals is presented in the below table:

Design Goal	Advantage Towards Security and Manageability
Provision of end to end WLAN Connectivity	Access Points with suitable RF Propagation strength are selected in a way that they can provide the connectivity to each of the client in the entire campus to provide each of them uninterrupted services of WLAN and also no one left un-located unless they turned their WiFi equipped devices turned off.
Support for Exponential Growth	Proposed technique has the ability to incorporate more then 10 LWAP and hundreds of WLAN users in it with complete provision plus protection of WLAN users' location information. This is achieved by selection of adequate WLC and Aggregation switch with POE support.
Provision of Robust Security	Cisco WLAN Controller is selected that has the capability of providing robust security mechanism for WLAN communication, prevention of un-authorized access and complete management of LWAPs and WLAN Clients. It has been achieved by the selection of APs and IOS which updates the Autonomous APs to LWAP which only

	listens to their Controller (WLC).
Secured Database Repository	Not completely but we have built our database repository system in a way that it can easily prevent adversary to access the database of user's location information. It has been achieved by the selection of advance protected Microsoft Server 2008 R2 with Update Service Pack and designing a Middleware Application that is responsible of protecting the information of users from accessing by untrusted user.

Table 7: Analysis w.r.t Design Goals of Proposed Technique

6.3. Comparison of WLAN User Location Information Obfuscation by DMAS with Our Proposed Technique

In order to compare our proposed technique with the technique has been designed with the ultimate goal of preserving user location information by dynamically changing the MAC addresses of WLAN Clients on periodic basis [12] we presented the tabular comparison and pointed out the facts that are related to the DMAS technique and are then compared to our proposed technique:

DMAS Obfuscation Technique	**Client Server WLAN Privacy Technique**
Dynamic change of user's MAC increases the overhead on the complete Layer2 network environment as after each dynamic assignment all layer 2 terminals need to refresh their learned MAC tables w.r.t the changed MAC addresses. Hence cannot support in environments having high user density and growth also disrupt ongoing network communications.	As mentioned in section 6.2 our technique has the support of exponential growth with no overhead to existing network communication.

DMAC creates a security risk as changing MAC on dynamic basis does not allow application of MAC filtering within the Wireless / Wired LAN.	In section 6.2 we have guaranteed the provision of Robust Security, no un-authorized entity can have the access to our Wireless LAN / WAN infrastructure, hence enabling higher level of security even at layer 2.
DMAC allows more chances to an adversary to get the access of network by using anonymous / un-real MAC address (by MAC Spoofing) and endanger user's privacy, critical information etc.	Our technique does not allow any DMAC, if even a valid user changes his/her MAC and tries to get access to our network will be blocked at layer2, hence no user un-identified MAC can enter into the network.
DMAC technique only provides the privacy of user location information in WLAN, the drawback is that in most cases it becomes necessary to detect WLAN Users and also prevent some of them from being detected which is not possible in this technique.	With reference to the section 5.3.7 we have developed an architecture which supports both prevention and provision of location information, and this technique can be customized on demand basis.

Table 8: Comparison Matrix of Proposed Technique with DMAS Obfuscation Technique

6.4. Summary

This chapter summarizes the complete research with its analysis and its comparison with another technique intended to prevent the user location information from being shared by an adversary. We have concluded this by comparing the grade of security and flexibility in our proposed technique which is much higher than the compared technique.

7. Conclusion and Future Work

7.1. Overview

In this technology world where there is a huge demand of Location Based Services that required their user to share the location information wanted / unwanted we have taken a one step ahead to provide a solution for WLAN users to get located / or prevented from being detected.

This chapter concludes the report providing a direction for future work.

7.2. Conclusion

In this complete report we started with the basic concepts of WLAN standards, how, where and when they are used in this 3rd generation era and pointed out the benefits of its utilization. Several methods of WLAN deployment, its models and the area of their applications which then turned its way towards the WLAN location detection through the use of WLAN infrastructure. In this report we have described different types of Location Detection architectures in wireless domain and also discussed the architecture to which we have used for our research. This report also described the ongoing requirement of location prevention and how it can endanger any user who is unaware of this fact and are sharing their location information unnecessarily. This complete discussion ended up with the selection of architecture, compartmentalized study of the features, functionalities and requirement of each of the equipment used in this research, lastly implementation of the proposed technique and its analysis with one of the similar technique developed to prevent the WLAN user location information.

7.3. Future Work

We intend to carry out the real time implementation and integration of our proposed technique into an environment where there is a need to WLAN user location provision with prevention as well. We have intentions to develop a more secured and efficient location prevention and estimation system which will have automated Radio Map generation on the basis of the collected information from WLC and also it will

integrate the graphical representation based on the output generated by the middleware application. More secure and fine data collection technique will be implemented to collect meaningful information from WLC and represent them in a more effective way.

ANNEXURE ‘A’

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Data.OleDb;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

namespace MACSoft
{
    public partial class Form1 : Form
    {
        DataTable dt = new DataTable("AllWiFiMAC");
        DataTable dt2 = new DataTable("AllWiFiMAC");
        public Form1()
        {
            InitializeComponent();
        }

        private void tb1_TextChanged(object sender, EventArgs e)
        {
            if (tb1.Text.Length == 2)
                tb2.Focus();
        }

        private void tb2_TextChanged(object sender, EventArgs e)
        {
            if (tb2.Text.Length == 2)
                tb3.Focus();
        }

        private void tb3_TextChanged(object sender, EventArgs e)
        {
            if (tb3.Text.Length == 2)
                tb4.Focus();
        }

        private void tb4_TextChanged(object sender, EventArgs e)
        {
            if (tb4.Text.Length == 2)
                tb5.Focus();
        }

        private void tb5_TextChanged(object sender, EventArgs e)
        {
            if (tb5.Text.Length == 2)
                tb6.Focus();
        }

        private void tb2_KeyPress(object sender, KeyPressEventArgs e)
        {
            if(e.KeyChar==8)
                if (tb2.Text.Length == 0)
                    tb1.Focus();
        }
```

```
        private void tb3_KeyPress(object sender, KeyPressEventArgs e)
        {
            if (e.KeyChar == 8)
                if (tb3.Text.Length == 0)
                    tb2.Focus();
        }

        private void tb4_KeyPress(object sender, KeyPressEventArgs e)
        {
            if (e.KeyChar == 8)
                if (tb4.Text.Length == 0)
                    tb3.Focus();
        }

        private void tb5_KeyPress(object sender, KeyPressEventArgs e)
        {
            if (e.KeyChar == 8)
                if (tb5.Text.Length == 0)
                    tb4.Focus();
        }

        private void tb6_KeyPress(object sender, KeyPressEventArgs e)
        {
            if (e.KeyChar == 8)
                if (tb6.Text.Length == 0)
                    tb5.Focus();
        }

        private void button1_Click(object sender, EventArgs e)
        {
            if (tb1.Text.Trim() != "" && tb2.Text.Trim() != "" &&
tb3.Text.Trim() != "" &&
                tb4.Text.Trim() != "" && tb5.Text.Trim() != "" &&
tb6.Text.Trim() != "")
            {
                statusbar.Text = "";
                //Change all textbox to uppercase before store to
variable
                tb1.Text = tb1.Text.ToUpper();
                tb2.Text = tb2.Text.ToUpper();
                tb3.Text = tb3.Text.ToUpper();
                tb4.Text = tb4.Text.ToUpper();
                tb5.Text = tb5.Text.ToUpper();
                tb6.Text = tb6.Text.ToUpper();

                //This variable will use for comparing with other MAC
to search critical user
                string chk_val = tb1.Text + ":" + tb2.Text + ":" +
tb3.Text + ":" + tb4.Text + ":" + tb5.Text + ":" + tb6.Text;
                //CHEKING OF CRITICAL MAC ADDRESS
                int found = 0;  //FLAG FOR CRITICAL MAC; 1 IF FOUND,
0 OTHERWISE
                string testval;
                for (int i = 0; i < dataGridView2.RowCount; i++)
                {
                    testval =
Convert.ToString(dataGridView2.Rows[i].Cells[0].Value);
                    testval = testval.Trim();
                    if (chk_val.Equals(testval) == true)
                    {
```

```
                        found = 1;
                        break;
                    }
                }
                //IF MAC ADDRESS FOUND IN CRITICAL LIST THEN SHOW
RANDOM VALUE
                if (found == 1)
                {
                    RANDFUNC:
                    Random random = new Random();
                    int randomNumber = random.Next(0,
dataGridView1.RowCount-1);

if(chk_val.Equals(Convert.ToString(dataGridView1.Rows[randomNumber].C
ells[0].Value).Trim())==true)
                        goto RANDFUNC;
                    statusbar.Text = "MAC : " + chk_val +
                                     "     RSSI : " +
dataGridView1.Rows[randomNumber].Cells[1].Value +
                                     "       LWAP Name : " +
dataGridView1.Rows[randomNumber].Cells[2].Value;
                }
                //IF MAC ADDRESS NOT FOUND IN CRITICAL LIST THEN SHOW
ACTUAL VALUE
                else
                {
                    for (int i = 0; i < dataGridView1.RowCount; i++)
                    {
                        testval =
Convert.ToString(dataGridView1.Rows[i].Cells[0].Value);
                        testval = testval.Trim();
                        if (chk_val.Equals(testval) == true)
                        {
                            statusbar.Text = "MAC : " + chk_val + "
RSSI : " +

Convert.ToString(dataGridView1.Rows[i].Cells[1].Value) +
                                  "       LWAP Name : " +
Convert.ToString(dataGridView1.Rows[i].Cells[2].Value);
                            break;
                        }
                    }
                    if(statusbar.Text=="")
                        statusbar.Text = "MAC address not found";
                }
            }
            else
                statusbar.Text = "Please enter valid MAC address";
        }

        private void Form1_Load(object sender, EventArgs e)
        {
            try
            {
                //FILE PATH
                string filepath = Environment.CurrentDirectory +
"\\all mac.xlsx";

                //PROVIDER COMMAND FOR XLSX FILE (2007 FORMATE)
                string connstr =
string.Format("Provider=Microsoft.ACE.OLEDB.12.0;Data
```

```
Source={0};Extended Properties=\"Excel 12.0 Xml;HDR=YES;IMEX=1\";",
filepath);
                OleDbConnection conn = new OleDbConnection(connstr);
                conn.Open();

                //DATA ADOPTER
                OleDbDataAdapter da = new OleDbDataAdapter();

                //STRING FOR QUERY
                string query = "select * from [AllWiFiMAC$]";

                //RUN QUERY
                OleDbCommand selectCMD = new OleDbCommand(query,
conn);

                //STORE DATA TO DATA ADOPTER
                da.SelectCommand = selectCMD;
                da.Fill(dt);

                //FILL DATA TO DATA GRIDVIEW
                //THIS WILL STORE THE FULL LIST OF USER'S MAC
                dataGridView1.DataSource = dt;
                conn.Close();

                //-------------------------------------------------
------------------------------
                //ANOTHER GRIDVIEW WILL CREATED AND SAME PROCESS AS
ABOVE
                //-------------------------------------------------
------------------------------
                //FILE PATH
                filepath = Environment.CurrentDirectory + "\\critical
mac.xlsx";

                //PROVIDER COMMAND FOR XLSX FILE (2007 FORMATE)
                connstr =
string.Format("Provider=Microsoft.ACE.OLEDB.12.0;Data
Source={0};Extended Properties=\"Excel 12.0 Xml;HDR=YES;IMEX=1\";",
filepath);
                OleDbConnection conn2 = new OleDbConnection(connstr);
                conn2.Open();

                //DATA ADOPTER
                OleDbDataAdapter da2 = new OleDbDataAdapter();

                //STRING FOR QUERY
                query = "select * from [AllWiFiMAC$]";

                //RUN QUERY
                OleDbCommand selectCMD2 = new OleDbCommand(query,
conn2);

                //STORE DATA TO DATA ADOPTER
                da2.SelectCommand = selectCMD2;
                da2.Fill(dt2);

                //FILL DATA TO DATA GRIDVIEW
                //THIS WILL STORE THE FULL LIST OF USER'S MAC
                dataGridView2.DataSource = dt2;
            }
            catch(Exception en)
```

```
            {
                MessageBox.Show(en.ToString());
            }
        }

        private void dataGridView1_CellContentClick(object sender,
DataGridViewCellEventArgs e)
        {

        }
    }
}
```

BIBLIOGRAPHY

[1] Karamtot. Krishna Naik and M.N. Giri Prasad, A System for Locating Users of WLAN using Dynamic Mapping in Indoor and Outdoor Environment-LOIDS Sree Visvesvaraya institute of Technology & Science, Mahabubnagar, India JNTU College of Engineering, Pulivendula, India 2008.

[2] Sara Nasre Wireless Lan Security Research Paper IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004.

[3] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing Wireless Location Privacy Using Silent Period, Nokia Research Center Japan, Arco Tower 17F, 1-8-1, Shimomeguro, Meguro-ku, Tokyo, 153-0064, Japan, +81-3-5437-3613 Institute of Industrial Science, University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo, Japan 2005.

[4] Christian S. Jensen, Hua Lu, and Man Lung Yiu, Location Privacy Techniques in Client-Server Architectures Google Inc., Mountain View, CA 94043, USA Department of Computer Science, Aalborg University, Denmark 2009.

[5] Jie Bao, Haiquan Chen, Wei-Shinn Ku, PROS: A Peer-to-Peer System for Location Privacy Protection on Road Networks (Demo Paper), Dept. of Computer Science and Software Engineering Auburn University 2009.

[6] ANQI LUO and LEIGE, Indoor Location Detection using WLAN, KTH Information and Communication Technology Master of Science Thesis Stockholm, Sweden 2009.

[7] Ling Liu, Bhuvan Bamba, Bugra Gedik, Peter Pesti, Ting Wang, From Data Privacy to Location Privacy: Models and Algorithm, Distributed Data Intensive Systems Lab College of Computing Georgia Institute of Technology 2007.

[8] Claudio Agostino Ardagna, Marco Cremonini, Gabriele Gianini, Landscape-aware location-privacy protection in location-based services, University of Milan, Department of Information Technology, via Bramante 65, 26013 Crema (CR), Italy.

[9] Hidetoshi Kid, Yutaka Yanagisawa, Tetsuji Satoh, Protection of Location Privacy using Dummies for Location-based Services, Graduate School of Information Science and Technology, Osaka University, NTT Communication Science Laboratories, NTT Corporation.

[10] Jafar Haadi Jafarian, A Vagueness-based Obfuscation Technique for Protecting Location Privacy, IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, Network Security and CERT Center Department of Computer Engineering Sharif University of Technology Tehran, Iran 2010.

[11] C.A. Ardagna, M. Cremonini, E.Damiani, S. De Capitani De Vimercati and P. Samarati, Location Privacy Protection Through Obfuscation-Based Techniques, Departmento di Technologic dell' Infermazione Universita di Milano 2007.

[12] Ming Lei, Xiaoyan Hong, Susan V. Vrbsky, Protecting Location Privacy with Dynamic Mac Address Exchanging in Wireless Networks. Department of Computer Science, University of Alabama Tuscaloosa, AL 35487-0290, 2007.

[13] Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode, Cisco Systems Inc. April 24 2008.

[14] Cisco Wireless LAN Controller Configuration Guide, Cisco Systems Inc. June 2010.

[15] K.Krishna Naik "Antenna Design Analysis, Construction and Testing for IEEE802.11 WLAN Range Improvements"- M.Tech Thesis at IIIT-Allahabad-2004.

[16] Neeli Prasad and Anand Prasad "WLAN System and Wireless IP for next generation communication".

[17] IEEE 802.11b Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[18] Moustafa Youssef, Ashok Agrawala, A. Udaya Shankar, "WLAN Location Determination via Clustering and Probability Distributions," IEEE Intnl. Conf. on Pervasive Comp. andComm. (PerCom) 2003, March 23-26, 2003.