Analysis of Inter Wi-Fi Access Points
Seamless Mobility

Ubaid ur Rehman
Spring, 2010

Master of Science Thesis
Stockholm, Sweden 2010

TRITA-ICT-EX-2010:167
Analysis of Inter Wi-Fi Access Points Seamless Mobility

Ubaid ur Rehman

Master of Science Thesis, 2010
Royal Institute of Technology (KTH), Stockholm, Sweden
Analysis of Inter Wi-Fi Access Points Seamless Mobility

Ubaid ur Rehman

uurehman@kth.se

June 2010

Examiner and Academic advisor: Markus Hidell, KTH, Stockholm, Sweden

Industry advisor: Olivier Marcé, Alcatel Lucent Bell Labs, Nozay, France.
Preface

The work depicted in this report was carried out at Alcatel-Lucent Bell Labs, Nozay, France. The project has two main goals. The first goal is to take measurements of Wi-Fi Access Points by warwalking in different sites of Paris. Then we analyze the collected data. To provide seamless mobility, it is important to know the Wi-Fi coverage of the deployed network. For this purpose, the focus of the second goal is to find out the average number of Access Points per scan, the distribution of the Access Points according to the signal strength, channels utilization, the time duration of each Access Point seen, and the Access Points deployed by different operators. Finally, we will investigate the possibilities for seamless mobility based on our analysis, observations, measurements and results. This report is submitted to Alcatel-Lucent Bell Labs, Nozay, France and Royal Institute of Technology, Stockholm, Sweden as partial fulfillment of the requirements for the Master of Science degree in Internetworking.
Acknowledgement

It is an honor and pleasure to express my cordial gratitude to my industry advisor Olivier Marce at Alcatel Lucent Bell Labs Nozay, France for his endless support, coordination and guidance throughout the various phases of the project. I am thankful to him for giving me the opportunity to work under his supervision. It would be a very challenging task to complete this project successfully according to the time plan. He pointed me out the right tools and techniques at every stage of the project. His valuable comments and feedback were of great importance. He provided critical and useful suggestions on how to solve a research problem systematically and thoughtfully. His continuous motivation, encouragement and support made me able to work and enjoy my stay in Alcatel Lucent Bell Labs. I admire other members and colleague of Triple play Wireless Network (TWN) department in Alcatel Lucent Bell Labs for their guidance, support and useful discussion. The friendly environment in Alcatel Lucent Bell Labs made me feel relax and comfortable during the project.

I would also like to thank my academic advisor Markus Hidell for his coordination and cooperation during this project. I convey my special admiration to Program Director Peter Sjodin and Program Coordinator May-Britt Eklund Larsson for their support during my MS at KTH. I am very grateful to all my friends for their advices and assistance.

Finally, I express special gratitude to my wife for being the best friend and holding my hand during the ups and downs of my life. Also my family, relatives and friends in my home country Pakistan deserve special credit for their encouragement. Specially, I thank my parents for their day and night prayers, motivation and inspiration throughout my whole life. They taught me in the best way to make me a good human being.
Abstract

Wi-Fi (WLAN/IEEE 802.11) has become one of the most popular user access technologies for its high bandwidth and low cost. Wi-Fi provides ubiquitous networks to nomadic users any time and any location. Nowadays, Wi-Fi has been deployed in most of the shopping malls, railway stations, airports, public libraries, cafeterias, hotels and many other public places. It is also widely deployed at homes thanks to DSL modem that include Wi-Fi. These resources can be reutilized by customers who are visiting such places. They can have the Internet services while on the move. As the Wi-Fi technology has very limited coverage, therefore a fast and smooth handover is very important for seamless session mobility of delay sensitive applications like VoIP (Voice over IP), online gaming, conferencing and real time video streaming. In this article, we present our results computed from data which was collected at different sites in Paris city. The objective is to assess if a mobile service could be offered based on the existing coverage. We then focus on computing the average number of APs (Access Points) in each dataset, measure the signal strength of APs, number of candidate APs, channel utilization, status of APs deployed by operators and observe the possibilities for a fast and seamless handover. Finally based on our analysis, observations and results, we will investigate that fast handover and seamless mobility in such environments is possible or not.
Sammanfattning

Contents

Preface .......................................................................................................................... 3
Acknowledgement ......................................................................................................... 4
Abstract ........................................................................................................................ 5
Sammanfattning ............................................................................................................. 6
Contents .......................................................................................................................... 7
List of Figures ................................................................................................................ 8
List of Tables .................................................................................................................. 9

1 Introduction ................................................................................................................ 10
   1.1 General Overview ................................................................................................. 10
   1.2 Context and Motivation of Work ........................................................................ 11

2 Overview of Wi-Fi Technology .................................................................................. 12
   2.1 IEEE 802 Network Technologies ....................................................................... 14
   2.2 Wi-Fi Architecture ............................................................................................. 15

3 Handover Mechanism ............................................................................................... 17
   3.1 Roaming in Wi-Fi ................................................................................................. 20
      3.1.1 Layer 2 Handover ....................................................................................... 21
      3.1.2 Layer 3 Handover ....................................................................................... 24

4 Media Independent Handover (MIH) IEEE 802.21 ............................................... 29
   4.1 MIH Objectives ................................................................................................... 29
   4.2 MIH Overview ..................................................................................................... 30
   4.3 MIH Services ....................................................................................................... 31
      4.3.1 Media Independent Event Services (MIES) ................................................ 32
      4.3.2 Media Independent Command Service (MICS) ......................................... 32
      4.3.3 Media Independent Information Service (MIIS) ......................................... 33

5 Art of Wardriving ....................................................................................................... 34
   5.1 Methodology ........................................................................................................ 35
   5.2 Analysis ................................................................................................................ 36
      5.2.1 Access Points Statistics ................................................................................ 38
      5.2.2 Candidate APs ............................................................................................. 41
      5.2.3 APs Deployed by Operators ........................................................................ 44
      5.2.4 Channels Utilization ..................................................................................... 44
      5.2.5 APs Seen for Specific Time Duration .......................................................... 45

Evaluation ..................................................................................................................... 47
Conclusion ...................................................................................................................... 48
Future Work ................................................................................................................... 49
References ..................................................................................................................... 50
APPENDIX A .................................................................................................................. 53
List of Figures

Figure 1.1 - Mobile Node performing handover .......................................................................................... 11
Figure 2.1 - Speed vs Mobility in different wireless technologies ................................................................. 12
Figure 2.2 - IEEE 802 family and it's relation to OSI model ........................................................................ 15
Figure 2.3 [12] - PHY components ........................................................................................................... 15
Figure 2.4 - Wi-Fi Architecture .................................................................................................................. 16
Figure 3.1[17] - Handover process based on signal strength ........................................................................... 18
Figure 3.2 [32] - Authentication, association and QoS exchange process during handover ......................... 23
Figure 3.3 [36] - Protocol messages exchange for handing over between APs in an IEEE 802.11r enabled WLAN ........................................................................................................................................ 24
Figure 3.4 [36] - CAPWAP architecture, an initial authentication followed by a handover of an MN from one WTP to another ........................................................................................................ 26
Figure 3.5 [36] - HOKEY, authentication and re-authentication in the visited network ................................. 27
Figure 4.1 - MIH/IEEE 802.21 architecture ................................................................................................. 30
Figure 4.2 - Communication between local and remote entities .................................................................... 32
Figure 5.1 - Example Map of Wi-Fi in Seattle ............................................................................................... 35
Figure 5.2 - Site A warwalking track .......................................................................................................... 36
Figure 5.3 - Site B warwalking track .......................................................................................................... 38
Figure 5.4 - Site A APs coverage with SNR=min and SNR>=30dB ................................................................. 40
Figure 5.5 - Site A APs coverage with SNR=min and SNR>=33dB ................................................................. 40
Figure 5.6 - Site B APs coverage with SNR=min and SNR>=30dB ................................................................. 41
Figure 5.7 - Selection Process of Candidate APs .......................................................................................... 42
Figure 5.8 - Site A number of candidate APs with SNR>=30dB and SNR>=33dB ......................................... 43
Figure 5.9 - Number of APs seen for specific time duration at site A ............................................................ 45
Figure 5.10 - Number of APs with SNR distribution at site A ...................................................................... 46
List of Tables

Table 2.1 - Comparison of IEEE 802.11 Standards ...................................................................................... 14
Table 5.1 - Summarized information collected by students in Seattle University........................................ 34
Table 5.2 - WIGLE database information ........................................................................................................ 35
Table 5.3 - Access points statistics from site A ................................................................................................. 39
Table 5.4 - Access points statistics from site B ................................................................................................. 39
Table 5.5 - Summary of candidate APs .............................................................................................................. 43
Table 5.6 - Wi-Fi coverage by operators with SNR>=30dB ............................................................................. 44
Table 5.7 - Percentage (%) of channels utilization............................................................................................ 44
1 Introduction

1.1 General Overview

The Internet has become an important part of our lives. Everyone wants the Internet while at home, office, shopping mall, airport, railway station, public library, hotel etc. Due to high demand of the Internet, Wi-Fi (IEEE 802.11/WLAN) [1] has become one of the most popular user access technologies for its high bandwidth, low cost and easy deployment. Originally, Wi-Fi was designed as a wireless network solution for indoor environments to avoid the complexity of wires among network devices. That is why, at that time handover from one AP to another AP was not considered as an important factor. Unlike the wireless internet services based on cellular technology, Wi-Fi can provide high speed Internet services up to 11 Mbps (IEEE 802.11b [2]) or 54 Mbps (IEEE 802.11a/g [3, 4]). Facing an increased user demand for the Internet services, service providers are offering services through different technologies. In the next generation of wireless communication different technologies are expected to integrate in order to provide universal wireless access with seamless mobility. The demand for Wi-Fi connections has increased exponentially. So the Wi-Fi has been deployed in most of the homes, offices, shopping malls, railway stations, airports, hotels, libraries and many public places. One can easily find many numbers of APs while being in such places. These resources can be reutilized by customers who want the Internet services, as long as there exists an agreement between customer and provider as FON (Foneros) [5] does. The classical IEEE 802.11 Wi-Fi does not support differentiated services and the traffic is equally treated as best effort. This makes it unable for Wi-Fi to support delay sensitive applications because of their QoS (Quality of Service) requirements. To support QoS features in Wi-Fi, some enhancements like IEEE 802.11e were made in the standard. This feature caused increase number of exchange messages between Mobile Node (MN) and AP. As a result the handover time is increased to an unacceptable level. The end user will experience poor quality of service.

Wi-Fi technology has very limited coverage area and MN has to perform handover very frequently. Therefore a fast and smooth handover is very crucial to keep session mobility for delay sensitive applications like VoIP, conferencing, live streaming, etc. Currently, handover time between different APs is one of the most important issues to be tackled in Wi-Fi in order to offer seamless mobility. In fast roaming [6], an MN seamlessly disassociates from one AP and associates to another AP without loss of connectivity as presented in Figure 1.1. For this process to be achieved, the deployment of such APs needs to be overlapped in coverage at the borders which gives an MN the ability to receive acceptable signal strength from another AP while it is still connected with its current one. There are two main steps involved in handover process: i) AP discovery and selection ii) Handover preparation and performing. In first step, the MN starts scanning for available APs in the surrounding. After completing scan, it selects a target AP based on its association and strongest signal strength of AP to handover to. In second step, MN starts preparation to handover. Finally, MN performs handover to the target AP. To achieve seamless mobility in Wi-Fi networks, the time taken by these two steps must be minimized as much as possible.

Paris is one of the biggest cities in Europe. On one side this beautiful city is full of history, culture and civilization. On the other side it is covered by Wi-Fi APs. In this city, the Wi-Fi APs have been deployed enormously in urban areas. In this project, we are going to analyze the Wi-Fi APs in different sites of Paris city. We will collect some data by warwalking at different locations. After collecting data, we will perform some computation to identify key parameters to determine the quality of Wi-Fi coverage: the average number of APs, their signal strength, duration of each AP seen and channel utilization. Finally we will evaluate the possibilities for seamless mobility based on our analysis, measurements, observations and results.
1.2 Context and Motivation of Work

In Paris Wi-Fi has been widely deployed in many places like homes, offices, airports, railway station, shopping malls, cafeterias, and public hotspots. The reasons for this rapid change are; Wi-Fi is cheap, easy to deploy, monitor, manage and extend, flexible and provides mobility to end users with high bandwidth. There are many operators like FON [5], Free [7], and Orange [8] etc which are playing a key role in deploying Wi-Fi infrastructure in this city. These operators have deployed their APs in many urban areas. If a customer has an agreement with any of these operators, he/she can use the services at any hotspot where these operators provide services like FON, Free, etc. So the theme of the project is to analyze the deployment of Wi-Fi APs in Paris city and to assess the possibilities to reutilize these resources by the customers who have an agreement with these operators. Is there any possibility for the customers to enjoy continuous services with seamless mobility while roaming in the city? Is there enough Wi-Fi coverage in the city? Answering these questions need to address some other ones. What is the average number of APs per scan? How the APs are distributed according to signal strength? What is the channel utilization? What is the status of operators deployed APs? What methodology and mechanism can be used to achieve these goals?

![Mobile Node performing handover diagram](image)

**Figure 1.1 - Mobile Node performing handover**
Overview of Wi-Fi Technology

Since last few years, the world has become increasingly mobile [9]. With the wired network, an end user cannot move from one place to another being connected to the Internet. The end user has to disconnect from the wired network in one place and reconnect to the wired network in another place. Wireless networks, however, poses no such restriction and allows the network users to move freely inside the domain. As a result, nowadays wireless technologies are more popular and demanding than traditional "fixed" or "wired" networks. In fact, today wireless interfaces are available to utilize network services that allow users to use e-mail and access applications, and browse the Internet from anywhere and anytime. These wireless applications are enabling people to extend their workplace in a way that results in significant benefits. Business travelers, for example, are able to respond to e-mails while waiting for a flight at an airport. A homeowner can easily share a common Internet connection among multiple PCs, laptops and other Wi-Fi enabled devices without using cables.

Similarly Wireless telephony has been successful because it enables people to connect with each other regardless of location. New technologies targeted at computer networks promise to do the same for the Internet connectivity. The most successful wireless networking technology so far has been IEEE 802.11. The Figure 2.1 [10] shows the graph for speed (bandwidth) and mobility for different wireless technologies. We can see that Wi-Fi offers very high bandwidth but with very low mobility.

![Figure 2.1 - Speed vs Mobility in different wireless technologies](image-url)
The initial IEEE 802.11 was published by Institute of Electrical and Electronics Engineers (IEEE) in 1997 and is known as IEEE 802.11-1997. This standard is now updated by the current standard IEEE 802.11-1999. The 1997 standard specified a bandwidth of 2 Mbps, with fallback to 1 Mbps in hostile environment. It supports two methods of encoding, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). IEEE 802.11 goes by a variety of names, depending on who is talking about it. Some people call “IEEE 802.11 Wireless Ethernet” (WLAN) to emphasize its shared lineage with traditional wired Ethernet (IEEE 802.3) [11]. It is also commonly referred as “Wi-Fi” (Wireless Fidelity). To help ensure Wi-Fi products perform correctly and are interoperable with each other, the Wi-Fi Alliance [12] was created in 1999. The Wi-Fi Alliance is a non-profit organization that certifies products conforms to the industry specification and interoperates with each other. Wi-Fi® is a registered trademark of the Wi-Fi Alliance and the indication that the product is Wi-Fi Certified™ signifies products have been tested and should be interoperable with other products regardless of who manufactured the product. Table 2.1 illustrates a basic comparison of different IEEE 802.11 standards. In this report, we will use “Wi-Fi” for IEEE 802.11/WLAN (Wireless Local Area Network).

Wi-Fi is a wireless communication system that allows hosts (computers/workstations) to transfer data with each other using radio waves as a transmission medium. Wi-Fi can be connected to a wired network or can operate independently by connecting several hosts wirelessly. Wi-Fi can provide almost all of the functionalities and high data transmission rates offered by wired LANs, but without the physical constraints of the wire itself. Wi-Fi configurations range from temporary independent connection between two computers to managed data communication networks that connect to other data networks like the Internet. Data rates for Wi-Fi system range from 1 Mbps to 54 Mbps. The enhancement in technology is aiming for 300 Mbps i.e. IEEE 802.11n [13]. Nowadays, this technology has an incredible demand in the market. Following are some reasons for this rapid growth in demand:

**Nomadic**

Wi-Fi provides the advantage of free movement to network users. They have the Internet connectivity and have access to all the resources while on the move.

**Roaming**

In Wi-Fi networks, a user can easily move from one network to another without any loss of the Internet connectivity.

**Ease and Speed of Deployment**

The deployment of Wi-Fi infrastructure is very easy and fast as compared to traditional fixed/wired LANs. It can be easily deployed in buildings, airports, railway stations, cafeterias, shopping malls and many other hotspots. In many cases, it is complicated to deploy a wired LAN e.g. a historical building or building with no blueprints. It also requires a lot of resources and very time consuming.

**Flexibility**

Wi-Fi networks provide great flexibility. It allows users to quickly form a small network for a meeting. You can move the network from one place to another with ease. No cables mean no re-cabling. Expansion to Wi-Fi networks is very easy as the network medium is already everywhere. There are no cables to pull, connect or plug. Flexibility is of high value in hotspots like rail stations, airports, shopping malls, cafes etc.

**Cost**

As Wi-Fi networks are easy to deploy and offer flexibility. So Deploying Wi-Fi infrastructure is very cheap as compared to fixed one. The Wi-Fi devices are getting cheaper day by day. In case of connecting two buildings, it is very easy and cheaper to bridge those with wireless network rather to lease a cable connection from service provider or deploy own wired network.

**Management**

It is very convenient to manage a Wi-Fi network as it is simple and straight-forward. There is no complexity of wires/cables in the network infrastructure.
Table 2.1 - Comparison of IEEE 802.11 Standards

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Bandwidth/Speed</th>
<th>Frequency Band</th>
<th>Maximum Indoor Range</th>
<th>Maximum Outdoor Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>1 Mbps</td>
<td>2.4 GHz</td>
<td>short</td>
<td>short</td>
</tr>
<tr>
<td>802.11a</td>
<td>54 Mbps</td>
<td>5 GHz</td>
<td>~ 50 feet</td>
<td>~ 100 feet</td>
</tr>
<tr>
<td>802.11b</td>
<td>11 Mbps</td>
<td>2.4 GHz</td>
<td>~ 150 feet</td>
<td>~ 300 feet</td>
</tr>
<tr>
<td>802.11g</td>
<td>54 Mbps</td>
<td>2.4 GHz</td>
<td>~ 150 feet</td>
<td>~ 300 feet</td>
</tr>
<tr>
<td>802.11n</td>
<td>600 Mbps</td>
<td>5 GHz and/or 2.4 GHz</td>
<td>~ 300 feet</td>
<td>~ 600 feet</td>
</tr>
</tbody>
</table>

2.1 IEEE 802 Network Technologies

Wi-Fi (IEEE 802.11) is a member of IEEE 802 family which is a series of specifications for Local Area Network (LAN) technologies. The Figure 2.2 [14] shows the relationship between the various components of the 802 family and their place in the OSI model. IEEE 802 specifications are focused on the two lowest layers of the OSI model because they incorporate both physical and data link components. All 802 networks have both a MAC and a Physical (PHY) component. The MAC is a set of rules to determine how to access the medium and send data, but the details of transmission and reception are left to the PHY. Individual specifications in the 802 series are identified by a second number. For example, 802.3 is the specification for a Carrier Sense Multiple Access network with Collision Detection (CSMA/CD), which is related to Ethernet, and 802.5 is the Token Ring specification. Other specifications describe other parts of the 802 protocol stack. IEEE 802.2 specifies a common link layer, the Logical Link Control (LLC), which can be used by any lower-layer LAN technology. Management features for 802 networks are specified in 802.1. Among 802.1’s many provisions are bridging (802.1d) and virtual LANs, or VLANs (802.1q) [14].

802.11 (Wi-Fi) is just another link layer that can use the 802.2/LLC encapsulation. The base of 802.11 specifications includes the 802.11 MAC and physical layers: a frequency hopping spread-spectrum (FHSS) physical layer and a direct-sequence spread-spectrum (DSSS) link layer. Later revisions to 802.11 added additional physical layers. 802.11b specifies a high-rate direct-sequence layer (HR/DSSS); products based on 802.11b. 802.11a and 802.11g describe a physical layer based on orthogonal frequency division multiplexing (OFDM). 802.11n describes a physical layer based on multiple input multiple output (MIMO).

The use of radio waves as a physical layer requires a relatively complex PHY, as well. 802.11 splits the PHY into two generic components: the Physical Layer Convergence Procedure (PLCP), to map the MAC frames onto the medium, and a Physical Medium Dependent (PMD) system to transmit those frames. The PLCP straddles the boundary of the MAC and physical layers, as shown in Figure 2.3. In 802.11, the PLCP adds a number of fields to the frame as it is transmitted “in the air” [14].
2.2 Wi-Fi Architecture

The Wi-Fi architecture is composed of several components and services that interact to provide connectivity and mobility to users. The Wi-Fi architecture is demonstrated in Figure 2.4.

**Station (STA):** Networks are built to transfer data between stations. A station is a basic component of Wi-Fi network. An STA is any device that provides IEEE 802.11 functionality and implements IEEE 802.11 medium access control (MAC) and physical (PHY) layers. These devices have wireless network interface card to communicate with each other. These devices include computers (desktop, laptops), PDAs, smart phones, mp3s, cameras, etc.

**Access Point (AP):** Frames on the Wi-Fi network must be converted to another type of frames for delivery on the wired network. Access points perform the wireless-to-wire bridging function. The AP is usually connected to a wired network and relay data between devices on each side of the bridge.

**Wireless Medium:** To transfer frames from one station to another, the technology uses wireless medium. The architecture allows multiple physical layers to be developed to support 802.11 MAC. Initially two radio frequencies (RF) physical layers and one infrared physical layer were standardized. Though the RF physical layers got far more popularity.

**Distribution System:** When several access points are connected to form a large coverage area, they must communicate with each other to track the movements of mobile stations. The distribution system is the logical component of 802.11 used to forward frames to their destination. IEEE 802.11 does not specify any particular technology for the distribution system. In most commercial products, the distribution system is implemented as a combination of a bridging engine and a distribution system medium, which is the backbone network used to relay frames between access points; it is often called simply the backbone network. In nearly all commercially successful products, Ethernet is used as the backbone network technology.
**Basic Service Set (BSS):** When two or more stations are connected and these stations communicate directly to each other, then this network is called Basic Service Set (BSS). This network is also called ad-hoc network. Such type of network is just for a short time and does not have any centralized management system.

**Infrastructure Basic Service Set (IBSS):** In this network, all the stations are connected to an AP. These stations communicate to each other via AP. The AP is connected to DS and is used to relay packets between stations.

**Extended Service Set (ESS):** When multiple infrastructure BSS are combined, they form an extended service set (ESS). The purpose of ESS is to provide greater mobility to stations. The stations can use the same layer 3 address and move from one IBSS to another. The frames are relayed between stations using APs via DS. The DS hides the mobility of the stations by treating the whole ESS as a single network (L2 domain).

**Service Set Identifier (SSID):** SSID is a unique tag that distinguishes one Wi-Fi from another. All APs and stations attempting to be part of the same Wi-Fi network must use the same SSID. Stations use this ID to be connected to an AP.

**Authentication Server (AS):** When stations try to connect to an AP, first must be authenticated by an AS. If the authentication is successful, the station is granted with access to network otherwise access is denied.

---

![Diagram](image-url)
3 Handover Mechanism

The handover is a process which refers to sequence of messages exchanged by APs and an MN resulting in a transfer of physical layer connectivity and state information from one AP to another. Thus handover is a physical layer process carried out by three participating entities namely the MN, old AP and new AP. The AP to which the MN had physical layer connectivity before the handover is the old AP while the AP to which the MN gets connectivity after the handover is the new AP. The state information that is transferred consists of client credentials and some accounting information. This transfer can be achieved by the Inter Access Point Protocol (IAPP) [15] or via a proprietary protocol such as Korean Telecom IAPP (KT-IAPP) [16]. There are two types of handovers:

i) Hard handover
In this type of handover, the MN is first disconnected from old AP and is then connected to new AP. This type of handover is also called ‘break before make’. There are some packets losses during this process and end users experience degraded quality of service.

ii) Soft Handover
To avoid the packet loss and experience good quality of service, the MN is first re-associated to new AP and is then disconnected from the old one. This kind of handover is also known as ‘make before break’.

In handover process there are also horizontal handover and vertical handover. When the handover is within technology (from Wi-Fi-to-Wi-Fi or form WiMAX-to-WiMAX) then such kind of handover is known as horizontal handover or intra-technology handover. But when the handover is between different technologies (from Wi-Fi-to-WiMAX or from GSM-to-Wi-Fi) then such handover is called vertical handover or inter-technology handover.

In Wi-Fi networks, an MN is connected to an AP. The coverage area of an AP is limited from 30 feet indoor to 600 feet outdoor. As the MN roams in the network, due to the limited coverage the MN is disassociated from old AP and is re-associated to a new AP. On the basis of Received Signal Strength (RSS) from current AP and neighboring AP, it is decided when to initiate this process. Figure 3.1[17] illustrates the result of signal strength propagation characteristics. When the MN moves away from AP1, its signal strength becomes weaker. Whereas the signal strength becomes stronger as it gets closer to AP2. By ignoring the geographic and environmental factors which affect the signal strength, we can find the average received signal over time.

There are four handover initiation techniques [17]:

- Relative Signal Strength
- Relative Signal Strength with threshold
- Relative Signal Strength with hysteresis
- Relative Signal Strength with threshold and hysteresis

Following we describe these four different handover initiation techniques briefly.

Relative Signal Strength
In this technique the handover is totally based on the received signal strength of an AP. Figure 3.1 describes that AP which has strong signal strength is preferred to handover because Received Signal Strength (RSS) is measured over time in relative signal strength. The Figure demonstrates that handover is requested at point A when the RSS of AP1 is decreased by RSS of AP2. In this scenario, many unnecessary numbers of handovers may be requested due to signal instability. Therefore, to reduce the network load unnecessary handovers should be avoided using handover techniques.

Relative Signal Strength with Threshold
Sometime the signal strength fluctuates and this fluctuation of signal strength may cause a station to swing back and forth between APs called Ping Pong effects [18]. To eliminate the ping-pong effects, the threshold value T is introduced with Relative Signal Strength as demonstrated in the Figure 3.1. When the Received Signal Strength value of AP1 is less than the Received Signal Strength value of AP2 and the RSS of AP1 is less than a threshold value T then the handover process is initiated.
Relative Signal Strength with Hysteresis

In this technique, Relative Signal Strength with Hysteresis introduces a value $h$ at point C as illustrated in Figure 3.1. Handover process is initiated when RSS of AP1 is less than RSS of AP2 and the RSS of AP2 is greater than the hysteresis value $h$ of AP1 at point C.

Relative Signal Strength with Threshold and Hysteresis

To minimize the number of handovers, the concept of threshold and hysteresis is combines in this technique. The handover process will be initiated at point C if the threshold value is less than $T_1$ but greater than $T_2$ and the RSS of AP2 is greater than the hysteresis value of $h$ of AP1 at point C.

![Figure 3.1[17] - Handover process based on signal strength](image)

In general the handover process can be explained as follow: initially an MN transmits and receives data by using old AP. When MN moves towards AP2 and detects low signal strength from old AP, it will start to explore other channels to discover new candidate APs for reconnection. By detecting a suitable new AP, the MN will attempt a re-authentication with that AP. If the authentication process is successful then MN will request a transfer association from old AP to new AP. After MN submits a re-association request to new AP, it waits for a response. If re-association request is successful then MN exchanges data through new AP. In brief, there are three (3) phases for a general handover process: a) Discovery phase b) re-authentication phase and c) re-association phase. These phases are explained as follow [19, 20].

**Phase I: AP Discovery**

When the RSS value of an AP is decreased to a certain threshold, the MN attempts to connect to a new AP. It starts AP discovery process by scanning neighboring APs. There are two types of scanning mode [21]: i) Active mode and ii) Passive mode. In fact, many vendors have preferred to deploy only the active discovery [22]. In active discovery, for each channel to scan, the STA sends a Probe Request and waits for a Probe Response from every reachable AP. The STA creates a report of all discovered APs and their characteristics. Then, the STA selects the more adequate AP to initiate next handoff phase. As it is shown in [16], several parameters control the discovery process: BSSType, BSSID, SSID, ScanType, ChannelList, ProbeDelay, MinChannelTime, and MaxChannelTime.

In active discovery, the number of channels selected for ChannelList defines two kinds of scans. The full-scan checks all usable channels and the short-scan that checks only a subset of the channel spectrum. Most mobile nodes use the following procedure for full or short scans [19]:

**Procedure:** Full or short scan in active discovery.
1: **For each** channel in ChannelList **do**,  
2: Tune the MN in channel to probe.  
3: MN waits for (channel activity detection) or (ProbeDelay timer expiration).  
4: **If** ProbeDelay expires, **then** channel is empty, probe the next channel.  
5: **If** channel activity is detected **then**  
6: MN gets access to wireless medium.  
7: MN broadcasts a Probe Request frame.  
8: MN waits MinChannelTime sensing the channel.  
9: **If** MN does not detect activity **then** probe next channel (not enough activity).  
10: **If** MN detects traffic **or** Probe Response **then**  
11: MN waits MaxChannelTime sensing the channel.  
12: **do** process any received Probe Response.  
13: **Until** MaxChannelTime expires, **then** probe next channel.

The channel switch and transmission latency is the time elapsed since the MN changes to the probe channel until the probe request frame is sent (lines 1-7). The MN broadcast a probe request and waits for MinChannelTime for a reply. On reception, the MN extends the sensing interval until MaxChannelTime to wait for more replies. If no reply is received in MaxChannelTime then next channel is scanned.

The number of channels to scan is the main contributing factor to discovery latency. Therefore a short-scan is preferred to a full-scan for fast handovers. However, the active discovery procedure may exhibit variable latencies due to the varying number of channels to scan and the variable time the MN stands on each channel [19].

In passive scanning mode, an MN listens to beacons frames broadcasted by APs and scans each channel of physical medium one by one. After scanning all the channels it will choose an AP based on its association and signal strength of beacon frames. Passive scanning is not appropriate for fast handovers.

**Phase II: Re-authentication**

In this phase, the MN authenticates with the target AP discovered in phase I. Authentication is a necessary prerequisite to association. However, IEEE 802.11 neither requires that authentication must be followed by association nor the authentication must immediately follow a channel scan cycle [19].

**Phase III: Re-association**

Re-association is the process for transferring associations from one AP to another. Once the MN is authenticated with the new AP, the association process can be started. According to [20] re-association process is a six steps process:

- Re-association request  
- Re-association response  
- Handover request  
- Handover response  
- Delivery of frames in buffer (optional)  
- Data transfer  

The re-association phase begins when MN switches to the new channel to issue a re-association request to the new AP. The MN’s request includes the current BSSID. New AP verifies the existence of a previous association between MN and old AP. If such association does not exist, the new AP de-authenticates the MN and the process ends. If previous association exist, then the new AP must locally decide if grants or not permission for re-association, notifying to the MN with a re-association response. Although IEEE 802.11 standard does not specify what factors shall be considered to take that decision, most AP manufacturers consider aspects like the number of MNs already associated to the new AP, the size of free buffers in the AP, and current traffic load in the
BSS. If permission is granted, the response message carries a success code and a value identifying the new association (AID), otherwise, the response message just carries the status code indicating the reason for denying permission. The new AP sends a Handover Request to the old AP. Then, old AP dissociates the MN from its associations table, update the new MN’s association, and send any temporally buffered packet to the new AP. Old AP returns a Handover Response and transfer any buffered frames to the new AP if they exist, so they can be delivered to the mobile node. Finally, the new AP begins processing frames for the recent associated MN.

To offer seamless mobility in Wi-Fi technology, we have to minimize the handover process time as much as possible. A significant delay is added by pre-handover steps (AP discovery and selection), authentication and then re-association to new AP, thus making it difficult to offer seamless mobility in Wi-Fi infrastructure. A new protocol mechanism was introduced by IEEE 802.21 called MIH (Media Independent Handover) which can assist the MN in handover process. In next section, Media Independent Handover (MIH) is explained in detail.

### 3.1 Roaming in Wi-Fi

Wi-Fi provides very high bandwidth with low cost. But the coverage area of Wi-Fi AP is limited to few hundred meters (300-600 meters). An MN has to perform frequent handovers while roaming around. The security provided by classical Wi-Fi as WEP (Wired Equivalent Protocol) was not well enough to rely on. The IEEE 802.11i was formulated to solve problems with original WEP encryption. It includes all the capabilities of WPA (Wi-Fi Protected Access) [23] and further defines a new encryption standard using AES-CCMP (Advanced Encryption Standard-Counter Mode using CBC-MAC Protocol). Both WPA and WPA2/802.11i support authentication through the 802.1X [24, 25] port-based method and share the key management techniques. The IEEE 802.1X port-based network access control mechanism to authenticate 802.11 mobile nodes was used as the authentication method. It is a layered security method of Authentication, Authorization and Accounting using the most common Remote Access Dial-In User Service (RADIUS) protocol [26]. The 802.1X standard lists EAP (Extensible Authentication Protocol) as authentication framework between the MN and the authentication server. EAP-TLS [27], EAP-FAST [28], EAP-SIM [29], and PEAP [30] are some of the EAP authentication methods that can be used, based on deployment credentials such as smart cards, PKI certificates, etc. With these advanced security mechanisms, the handover process became very complex and time consuming.

The BSS transition process where an MN roams from one AP to another could consist of up to 6 stages: discovery (Probe exchange), 802.11 open authentication, Re-association, Authentication method, EAPOL key exchange, and QoS renegotiation. This process is depicted in Figure 3.2 [32]. The 802.1X authentication frame exchange process encompasses the MN (supplicant) that sends access requests to the AP (authenticator) which controls the access to the network, and the authentication server which is the AAA/RADIUS server that provides the services for the authenticator by checking the credentials of the MN and authorizing the MN accordingly. The conversation usually consists of requests for authentication information by the radius server and responses by the MN. The Authentication Server and the mobile node would have agreed upon one set of Pairwise Master Keys (PMK), which is then distributed to the AP using RADIUS protocol. Both the MN and AP would use this PMK to mutually authenticate as well as derive a new set of Pairwise Temporal Keys (PTK) for encryption of data communication. This is followed by an EAPOL 4-way handshake between the MN and the AP to establish the keys [24, 31, 32].

Also the classical Wi-Fi does not support differentiated services and the traffic is equally treated as best effort. This makes it unable for Wi-Fi to support delay sensitive applications because of their QoS requirements. The IEEE 802.11e Task Group (TGr) [33] defined some amendments to support QoS in IEEE 802.11 MAC. As the original 802.11 MAC did not differentiate traffic to support delivery of delay sensitive packets. The 802.11e standard introduces a new Hybrid Coordination Function (HCF), which combines functions from Distributed Coordinated Function (DCF) and Point
Coordination Function (PCF) with enhanced QoS-specific mechanisms and frame formats. As Wi-Fi provides contention-based medium access, it was necessary to implement Admission Control mechanism to regulate traffic. The MN and AP negotiate the traffic specification during the QoS exchange process.

From the roaming perspective, the 802.11i and 802.11e standards introduce additional overhead during the re-authentication process due to multiple management frame exchanges. As the MN roams from one AP to next, it needs to perform full 802.1X re-authentication and this could take up to hundreds of milliseconds or even seconds to complete depending upon the authentication server load and traffic conditions. Such high latencies affect user experience on a voice over WLAN call. For example, a mobile node is running a VoIP call while performing handover from one AP to another. So to complete this complex process of re-authentication, re-association and QoS parameters negotiation will cause high delay. Thus the end user will experience an interruption in the VoIP communication. This will lead to a poor voice quality. To minimize these delays, PMK caching and pre-authentication mechanisms could be supported; but these methods do not scale well and have seen limited deployment support since they are optional. Hence, there was a need to formulate a standard mechanism by which the timing issues due to re-authentication, reauthorization and QoS renegotiation during roaming could be completely resolved to provide optimal user experience [32].

To solve this problem, three protocols Control and Provisioning of Wireless Access Point (CAPWAP) [34] by IETF CAPWAP Working Group (WG), Handover Keying (HOKEY) [35] by HOKEY WG and IEEE 802.11r Fast BSS Transition [31] were introduced. The purpose of these protocols is to maintain the features of IEEE 802.11i for security and IEEE 802.11e for QoS and minimize the delay during the handover process as much as possible. The mobile node should have a good voice quality while performing a handover from one AP to another. CAPWAP and HOKEY are being standardized by the Internet Engineering Task Force (IETF) in the form of request for comments (RFC). These protocols are under development phase till now. IEEE 802.11r is an amendment to the IEEE 802.11 standard and is therefore being completed by the IEEE in July 2008.

3.1.1 Layer 2 Handover

As mentioned in section 2.2 that Wi-Fi architecture is composed of Extended Service Set (ESS). Each ESS consists of one or more Basic Service Set (BSS). In each BSS, there are one or more APs, to which different MNs are connected and communicate via the AP. This whole setup is under one domain and is managed by one central administration. When an MN roams in this network, it uses one unique IP address for communication. Suppose an MN is connected to AP1 and starts roaming in the network. After moving a while, the signal strength of AP1 will become weaker due to Wi-Fi short range. At that point, AP2 will have stronger signal strength than AP1. Now the MN will try to connect to AP2 and will start the handover process. As this is a single domain, during this handover the MN will see no change at IP level. It will only change the point of attachment by disconnecting from AP1 and connecting to AP2. So this type of handover is known as L2 handover. The fast BSS transition (IEEE 802.11r) is a mechanism which works on layer 2 handover [36].

3.1.1.1 Fast Basic Service Set (BSS) Transition IEEE 802.11r

As mentioned before that original standard of IEEE 802.11 does not support QoS features and the traffic is treated as best effort. It was unable for IEEE 802.11 to run real time and delay sensitive applications. Also the security provided by IEEE 802.11 was not strong enough. So to cope with these issues, some additional features were added to the original standard, including IEEE 802.11e for QoS and IEEE 802.11i to strong the security in Wi-Fi infrastructure. With these features introduced in Wi-Fi technology, roaming in Wi-Fi networks became more complex and time consuming process and it is an important problem to be solved for real time applications. The IEEE 802.11r task group was thus formed to provide solutions to minimize the time taken for BSS transition process to support
real time and delay sensitive applications. The goal of the new initiative is to ensure to make the target AP ready for next roaming before the MN actually starts roaming.

In IEEE 802.11r, when the MN initially connects to an AP, it performs full EAP authentication process. Both the AP and MN are mutually authenticated. Fast BSS transition uses three levels key hierarchy. In IEEE 802.11r, the role of authenticator is divided into two different parts—the mobility domain controller (MDC) and the AP. The MDC is responsible to grant access to the network and the AP responsibility is to establish a secure channel with MN. After EAP authentication, a MSK (Master Session Key) is generated at both AAA server and MN. The AAA server transfers the MSK to MDC. The MSK is called root key in IEEE 802.11r. Then the first level key is generated from MSK at MN and MDC which is called Pairwise Master Key-R0 (PMK-R0). As the MDC holds the PMK-R0 key, so it is called R0 Key Holder (R0KH). The MDC will cache PMK-R0 and will use this key to derive session keys for other APs in the same mobility domain. When an MN handover from one AP to another, R0KH will generate a second level key (PMK-R1) from PMK-R0 and forward it to the new AP. This new AP is known as R1 Key Holder (R1KH). Each PMK-R1 is derived at the MDC for one specific AP and contains information about that AP. The PMK-R1 binds the AP into a secure channel to be generated. From PMK-R1 key Pairwise Transient Key (PTK) is derived which is the third level key in IEEE 802.11r key hierarchy. In IEEE 802.11r, when the handover occurs, the PTK can be generated by a modified authentication request/response messages exchange. These modified messages include the nonces and keying information to derive new PTK from the PMK-R1, thus avoiding the full IEEE 802.11i four-way handshake [37]. This process minimizes the latency resulted when an MN is connected to the back end system.

802.11r can establish a secure channel between the MN and the new AP very quickly, in one single round trip. It is faster than 802.11i, which requires four-way handshake. 802.11r supports both proactive and reactive handovers. However, 802.11r can be used only in intra-domain handovers because if the MN goes into a new domain, 802.11r does not have a mechanism to derive a new set of keys for the new domain other than a full authentication. 802.11r also requires a new key-distribution mechanism to distribute PMK-R1 to the new AP. This key-distribution mechanism is still undefined [36]. In 802.11r, PMK-R1s are distributed by PMK-R0KH. In a large network, this can result in a large signaling load at PMK-R0KH. If several PMK-R1s can be combined and distributed to the first PMK-R1KH and then distributed from that PMK-R1KH instead of PMK-R0KH, the signaling load at PMK-R0KH can be reduced [38]. Figure 3.3 [36] illustrates the IEEE 802.11r enables Wi-Fi architecture and the exchange of protocol messages between the APs.
Figure 3.2 [32] - Authentication, association and QoS exchange process during handover
3.1.2 Layer 3 Handover

In Wi-Fi architecture, a domain is a setup which is administered by one central authority. Each domain uses a specific IP subnet to be uniquely identified. Each device on the network has a unique IP address to communicate with other devices. Generally, when an MN moves from one domain to another it has to change the IP address (layer 3) in order to connect to the new network and start communication. Even in some mechanism like Mobile IP (MIP) [39], the MN can have the original IP address but in that case it uses a Care-of-Address (CoA) assigned by the new domain. In this report, we will not discuss those mechanisms. We will only explain the general layer 3 handover techniques. For example, an MN is connected to an AP in domain A. It starts roaming and after sometime it enters to the coverage area of AP2 which is the part of domain B. At this position, the signal strength
of AP1 is weaker than AP2; the MN will start handover process. In this situation, the MN will be disconnected from AP1 and connected to AP2. As AP2 is part of domain B, the MN will be assigned a new layer 3 IP address for communication with other devices. Therefore, such type of handover is known as Layer 3 handover. CAPWAP and HOKEY are mechanisms which can operate in same domains as well in different domains.

3.1.2.1 Control and Provisioning of Wireless Access Point (CAPWAP)

Large Wi-Fi deployments introduce several problems. As each AP has an IP address which requires configuration, management, monitoring and control. Also every AP’s configuration is almost similar to the next AP. So deploying Wi-Fi connections in large enterprises is a complex, confusing and tedious task for a network administrator. There is a need for a system/protocol which can be very helpful in such environments. The work group CAPWAP was thus formed by IETF to provide solutions to these problems. The purpose of CAPWAP is to provide a standard to support enterprise Wi-Fi environments, from corporate sectors to university campuses. This protocol assumes that all APs are managed by a central authority. In this architecture, the AP is divided into two logical components. A traditional “Fat AP” implements both the physical (PHY) and medium access control (MAC) layers of the IEEE 802.11 protocol. With CAPWAP, the PHY and lower portions of the MAC protocol are implemented in “Thin APs” called wireless termination points (WTPs), while the upper MAC functionality for all APs in the enterprise network is implemented by a centralized controller called the access controller (AC) [36].

After this division, the authentication and access control features of IEEE 802.11 resides in centralized AC. In CAPWAP, the AC acts as an authenticator and the AAA (Authentication, Authorization and Accounting) server has no knowledge of the split nature of Wi-Fi infrastructure. During the initial authentication process, the mobile node performs EAP (Extensible Authentication Protocol) authentication with AAA server according to IEEE 802.11i standard. Mobile node sends the messages to AC via WTP and then AC forwards these messages to AAA server and vice versa. Once the EAP process is completed, the resulting session key is handed over to AC by AAA server. Then AC performs the four-way handshake with mobile node. As a result, a traffic key is generated which is forwarded to WTP using CAPWAP protocol. The traffic key is used by WTP and MN to encrypt data communication. The mobile node can connect to any WTP without performing EAP re-authentication process to the AAA server. When a mobile node wants to handover from one AP to another, after completing the discovery phase, the AC performs a four-way handshake with mobile node. The resulting traffic key is delivered to WTP securely. There is no need to execute the EAP re-authentication with AAA server to derive a new session key. Thus in many environments we can minimize overall handover time by minimizing EAP re-authentication time. This whole process is demonstrated in Figure 3.4 [36].

3.1.2.2 Handover Keying (HOKEY)

Extensible Authentication Protocol (EAP) [40] is a general framework supporting multiple authentication methods. The primary purpose of EAP is to provide a network access control. In many common deployment scenarios, an EAP peer and EAP server authenticate each other through an authenticator. The authenticator does not participate in the EAP exchange and simply acts as a gateway between EAP peer and EAP server during the EAP method execution. Wireless handover between APs is a complex process and involves several layers of protocol execution. Often times executing these protocols results in unacceptable delays for many real time applications such as voice. One part of handover process is EAP re-authentication, which can contribute significantly to the overall handover time. Thus in many environments, we can lower overall handover time by lowering the EAP re-authentication time. In existing EAP implementations, when an MN joins a new AP, it executes full EAP re-authentication process irrespective of whether it has been authenticated recently or has an unexpired key [40]. Thus resulting in a longer handover time and the MN may experience poor quality of service.
1) Authentication of EAP method between MN and AAA server
2) Key distribution from the AAA server to the authenticator, the AC
3) Four-way handshake executed between MN and AC
4) CAPWAP Add-Mobile message from AC to WTP1 with traffic key
5) MN wishes to handover to WTP2; executes four-way handshake with AC via WTP2
6) CAPWAP Add-Mobile message from AC to WTP2 with traffic key
7) MN wishes to handover to WTP3; executes four-way handshake with AC via WTP3
8) CAPWAP Add-Mobile message from AC to WTP3 with traffic key

Figure 3.4 [36] - CAPWAP architecture, an initial authentication followed by a handover of an MN from one WTP to another
1) Execution of EAP method between MN and home AAA server
2) Key distribution from the AAA server to the AP1
3) Four-way handshake executed between MN and AP1
4) MN wishes to handover to AP2 in another domain; executes ERP with local AAA server
5) Local AAA server requests and receives a domain-specific re-authentication key
6) Local AAA server generates session key and delivers it to AP2
7) MN executes four-way handshake with AP2
8) MN wishes to handover to AP3; executes ERP with local AAA server
9) Local AAA server uses domain-specific re-authentication key to derive a session key for AP3, and delivers it
10) MN executes four-way handshake with AP3

**Figure 3.5 [36] - HOKEY, authentication and re-authentication in the visited network**

To solve these issues, IETF formed a working group called HOKEY. The aim of this working group is to design a protocol which supports a fast handoff from one AP to another and also can roam among different operators. HOKEY has extended the EAP to natively support the fast handover. The EAP Re-authentication Protocol (ERP) [40] allows an MN to use keys derived during the initial EAP authentication to derive a session key in one round trip re-authentication for a new AP. This AP then performs four-way handshake with the MN and generates the traffic keys. In HOKEY architecture, each AP is an independent authenticator and ERP allows the AAA server to generate different session keys for each AP without re-executing the full EAP authentication process. Another key feature of HOKEY is its ability to support roaming in another wireless domain. If two wireless networks have roaming agreement then an MN can connect to an AP of another network. In this
case, the visiting network AAA server will proxy the authentication of the MN to the home AAA server. In this scenario, HOKEY also supports fast re-authentication to the visited network. The local AAA server caches the authentication keys and it uses the keys to derive a new session key when the MN wants to handover from one AP to another in the visited network. HOKEY uses AAA protocol to deliver the keys from home AAA server to local AAA server. Rather than reusing any of the existing keys in the IEEE 802.11i keying hierarchy, HOKEY makes use of the extended master session key (EMSK), which is derived during the initial EAP authentication and until now unused. Part of the HOKEY group’s charter is to define a keying hierarchy based on the EAP EMSK that can be used for generating application-specific keys [41]. Keys are grouped into key management domains, each rooted by a domain-specific root key (DSRK) generated from the EMSK, and from the DSRK we can generate a handover root key (HRK) for re-authentication. Figure 3.5 [36] depicts this mechanism along with the messages exchanged between different APs.

In this section, we discussed different handover mechanism. In small to medium organizations, IEEE 802.11r can be implemented to provide fast re-authentication and re-association in order to minimize the overall handover delay. The problem with this mechanism is that it only works inside one domain. It cannot be implemented in inter-domain handover scenario. Also it has some scalability problems when distributing the keys to the new APs. The CAPWAP approach is better for large enterprises when there are many APs deployed. This mechanism works in intra-domain and inter-domain handover scenarios. In this approach, a logical distribution is required in each AP. The HOKEY also supports handover between different domains. It can also be implemented for medium to large enterprises. It depends on requirements and scenario to use one specific approach. But in our opinion, it is better to use either CAPWAP or HOKEY as both of these mechanisms support handover between different domains.
4 Media Independent Handover (MIH) IEEE 802.21

For the past few years, various wireless access technologies such as Global System for Mobile communications (GSM), Code Division Multiple Access 2000 (CDMA 2000), Universal Mobile Telecommunication System (UMTS), Wireless Local Area Networks (WLAN), and Worldwide Interoperability for Microwave Access (WiMAX) have enormously evolved and deployed in most parts of the world. The enhancement in data networks and wireless devices has made live streaming, multimedia entertainment and social networking a reality of today. New Internet applications and services are being introduced. Moreover, the users demand for higher service quality including higher data rate, higher mobility, and Quality of Service (QoS) have continuously increased these days. However, such user demands have not been fulfilled by any of the above mentioned wireless technologies alone. WLAN provides high data rates but with very low mobility. Similarly CDMA 2000 offers high mobility but very slow data rate. Device manufacturers are integrating more and more network interfaces into their devices. For example, many mobile handsets now support both Wi-Fi and 3G technologies like Apple iPhones, Nokia N97, HTC Magic etc. Notebooks are equipped with built-in Wi-Fi, 3G and WiMAX interfaces. As these devices with multiple interfaces continue, operators must have to offer easy access across their different wireless technologies to be used from one device. Today a big challenge for service providers is to offer a seamless mobility across heterogeneous wireless technologies with specified QoS features. Operators who have this ability can better manage their resources and better fulfill the service requirements of their valued customers. Therefore, beyond 3G or 4G networks are integrating those multiple heterogeneous wireless access technologies into a common convergence network [42, 43]. The key point of future convergence technologies is to provide ubiquitous networks to the valued customers. Such ubiquitous networks are expected to guarantee ‘any-service with any-device through any-network at any-place at any-time’. In order to support this ubiquitous service, there are crucial requirements which are very high data rate for ‘any-service’, multi-interface systems for ‘any-device’, integrated heterogeneous networks and high mobility for ‘any-network’, and so on. Consequently, it is essential that multi-interface systems roam seamlessly across heterogeneous wireless access networks [44].

The IEEE 802.21 is proposing the Media Independent Handover (MIH) Services to enhance the handovers across heterogeneous access networks, i.e. vertical handover, and to optimize the service (or session) continuity during handovers, i.e. seamless handover. For this reason, MIH provides generic link layer intelligence and other related network information to upper layers. Particularly, MIH offers a framework of the message flows between handover-related entities to provide information on handover candidate networks and to deliver handover commands [45, 46]. Figure 4.1 [47] illustrates the general architecture of MIH standard.

4.1 MIH Objectives

MIH is focused on the following main fundamentals [47]:

- A framework that enables seamless mobility in heterogeneous technologies. This framework is based on a protocol stack which is implemented in all devices involved in seamless mobility.
- The definition of a new link layer Service Access Point (SAP) that offers a common interface for link layer functions and is independent of the technology specifics.
- The definition of a set of handover enabling functions that provide the upper layers with the required functionality and information to perform handover.
- The service to be continued during and after the handover procedure. One of the goals to avoid the break in the service to allow seamless mobility.
The MIH framework provides necessary functions which make handover decisions based on QoS parameters. For example, we may decide to handover to a new network which guarantees the desired QoS.

The MIH framework provides applications with functions which are aware of the handover and participate in handover decision. For example, a voice application may decide to perform handover during the silent period in order to minimize service disruption.

The MIH feature that allows the users information about the candidate neighboring networks for handover.

Network selection is the process of making a handover decision based on several aspects (e.g., throughput, QoS, congestion, policies, billing etc). IEEE 802.21 will only provide the necessary information to assist network selection but does not make handover decisions which are the responsibility of higher layers.

MIH can also assist in power management. For example, power consumption can be minimized if the MN is informed of network coverage, optimal link parameters or sleep/idle modes.

---

**4.2 MIH Overview**

One way to ensure handover interoperability across multiple access technologies is to create multiple media specific extensions. Each specific access technology has to have different media specific extensions for every other technology to interoperate with each other. For example an access technology T1 could be extended to interoperate with access technology T2, whereas another extension would be required to ensure interoperability with access technology T3. Similarly access technologies T2 and T3 would require their own extensions. Continuing in this fashion requires \( N \times (N - 1) \) media-specific extensions to ensure that \( N \) access technologies all interoperate with each other. The complexity of this type of approach grows on the order of \( N^2 \) and does not scale well as more access technologies are considered and the system will become more and more complex [48].

A media independent framework is a more efficient and scalable method of addressing intertechnology handovers. With a common platform to address handovers, each access technology will require a single extension to ensure handover interoperability with all other access technologies. This approach will scale more efficiently than a media specific approach. This is the approach embraced by Media Independent Handover (MIH), which defines a common set of MIH services that interacts with the higher layers of the protocol stack. The MIH is unique within IEEE standards in that it provides interoperability within IEEE 802 systems (e.g., IEEE 802.11 and IEEE 802.16e) and

---

**Figure 4.1 - MIH/IEEE 802.21 architecture**
between IEEE 802 and non IEEE 802 systems (e.g. cellular networks). The need for MIH services spanning multiple external networks led to the creation of the IEEE 802.21 WG with a project to create a standard that “defines extensible 802 media access independent mechanisms that enable the optimization of handover between heterogeneous 802 systems and may facilitate handover between 802 systems and cellular systems” [49]. The aim of the MIH is to provide MIH functionality that facilitates fast and seamless handovers initiated by network or mobile node. The specification [45] consists of the following elements:

- **MIH Function (MIHF):** MIHF has three types of services:
  - The Media Independent Event Services (MIES) which detects any changes in link layer and reports appropriate events from both local and remote interfaces.
  - The Media Independent Command Services (MICS) provides a set of commands for both local and remote MIH users to control link state.
  - The Media Independent Information Services (MIIS) provides information about neighboring networks including their location, parameters, properties and related services.

- **Service Access Point (SAP),** which define both media specific and media independent interfaces. Some SAPs are defined below:
  - MIH_SAP, a media independent SAP that provides a common interface for higher layers to control and monitor different links regardless of access technology.
  - MIH_LINK_SAP, a media specific SAP that provides an interface for MIHF to control and monitor media specific links. For MIHF to provide MIES and MICS for a specific link layer, it must implement an MIH_LINK_SAP for that specific link layer.
  - MIH_NET_SAP, a media dependent SAP that provides transport services over the data plane on the local node, supporting the exchange of MIH information and messages with the remote MIHF.
  - MIH users, which are the functional entities that employ MIH services.

MIHF is a logical entity that provides abstract services to the higher layers through a media independent interface and obtains information from the lower layers through media specific interfaces. MIH services may be local or remote. Local operations occur within a protocol stack and remote operations occur between two MIHF entities.

### 4.3 MIH Services

The Media Independent Handover services provide generic link layer functionality and other related network information to upper layers. The goal is to enhance the mobile user experience by optimizing handovers between heterogeneous access networks. This includes different media types specified by Third Generation (3G) Partnership Project (3GPP), 3G Partnership Project 2 (3GPP2) and both wired and wireless media in the IEEE 802 family of standards. The MIH is an evaluation for all media, providing capabilities to detect and initiate handovers from one media to another (e.g. Wi-Fi to WiMAX or Wi-Fi to cellular). Such kind of handovers is known as vertical handover. It also offers solutions for service/session continuity to provide seamless mobility to end users. In order to offer seamless handovers, MIH provides information on potential candidate networks and delivers commands regarding handover. Furthermore, it reports dynamic events relating to link layer triggers, measurement reports, and timely indications of changes in link conditions. These roles speed vertical handovers while helping to keep end-to-end service continuity [45, 50].

MIH defines three main types of services with different associated entities to enable seamless mobility among heterogeneous technologies: MIES, MICS and MIIS. These services are controlled, managed and configured by another service called management service. The management service is responsible for MIH capability discovery, MIH registration, and MIH event subscription. Due to SAP and service primitives to higher layers, the MIHF enables applications to have a common interface across different media specific layers. Media specific SAPs (MIH_LINK_SAPs) enable the MIHF to obtain media specific information that can be delivered to MIH users using a single common interface (MIH_SAP). In the following section, MIH services are described briefly.
4.3.1 Media Independent Event Services (MIES)

The MIES defines events that represent changes in dynamic link characteristics such as link status and link quality. These events may indicate changes in the state and transition behavior of physical, data link and logical link of these layers e.g. Link_Up, Link_Down. Several entities could be interested in these events. The standard specifies a subscription mechanism. When the event is generated, it will be delivered to the subscription list. Events can be classified into two categories: link events that originate from lower layers and propagate to upper layers. MIHF events are originated from the MIHF and are propagated to MIH users which are subscribed for such events. Events can also be divided to either local events or remote events. Local events are subscribed to by local node. While remote events are subscribed to by remote node and these events are delivered over a network. For example, in case of local event, a Link_Up event generated from link layer is delivered to the MIH user of the same node. If a remote MIH user subscribed to this event, it is delivered to remote MIH user over the network as shown in Figure 4.2 [47].

4.3.2 Media Independent Command Service (MICS)

The MICS enable higher layers to control the lower layers to determine the status of links or control and configure the terminal or facilitate optimal handover policy [47]. The receipt of a certain command request may cause event generation. Commands can be classified into two categories: MIH commands which are invoked by MIH users and link commands which are generated by MIHF. Commands can also be divided into local commands and remote commands. Local commands propagate from MIH users to MIHF and then from MIHF to lower layers. While remote commands may generate from local protocol stack entity to the MIHF in peer protocol stack entity. Remote commands are carried by MIH protocol messages and can travel down to lower layers as link commands or go up to MIH users as MIH indications as depicted in Figure 4.2. The mobility management service should combine dynamic information about link status and parameters provided by MICS with static information regarding network status, network operators or high layers information provided by MIIS to help in handover decision.

Figure 4.2 - Communication between local and remote entities
4.3.3 Media Independent Information Service (MIIS)

The MIIS provides a framework through which an MIHF entity can discover and obtain network information existing within a geographic area to facilitate the handovers. The aim is to get knowledge about all heterogeneous networks in the area of MN to facilitate handover while MN is roaming to those networks. MIIS provides a set of information elements (IE), the information structure and its representation and a query/response type of mechanism for information transfer. IE provides information about lower layers such as neighbor maps, coverage area and other link parameters. Information related to upper layers such Internet connectivity in certain area or availability of certain services or load on the network etc can also be provided. MIIS is designed to provide information mainly about 802, 3GPP and 3GPP2 networks; however this list may be extended in future. All the information not only related to the technology to which the MN is currently attached but also to the surrounding technologies can be accessed from one single technology. For example, a mobile node currently attached to an 802 network such as Wi-Fi, will be able to collect information about other technologies like 3G cellular network within its geographic area without to power up its 3G interface to get this information. This characteristic allows optimal power utilization [47].

The MIH protocol assists the MN by providing the necessary information about the surrounding networks i.e. Wi-Fi, Wimax, and GSM etc. By using the provided information, a MN can decide when and to which AP it should perform handover and the MN will be able to have a seamless mobility. The MIH infrastructure is very beneficial for MNs but it is a complex protocol in terms of architecture and deployment. The MIIS has to be updated very frequently to know the current status of each network.

Normally, the AP selection is based on Strongest Signal Strength (SSS) which a simple mechanism based on the signal strength of an AP. This mechanism does not take into account other parameters like number of MNs connected to a specific AP, load on the AP, available resources, total capacity and channel utilization. In order to minimize the overall handover delay and consider these mentioned parameters for better performance and good quality of service, it is recommended to deploy IEEE 802.21 (MIH) architecture. But deploying IEEE 802.21 architecture is more complicated than SSS mechanism.
5 Art of Wardriving

The convenience of wireless networking has led to the widespread deployment of Wi-Fi APs in homes, offices, libraries, airports, railway stations, shopping mall and cafeterias etc. Some of these APs are managed by an administrator and are well secured. While many of these APs deployed in residential areas are installed as with default settings. Most commonly, the default settings disable wireless encryption. With some studies reporting as many as 50% of popular wireless APs deployed on default settings [51], ease of setup coincides with mass vulnerability.

Wardriving is the act of discovering Wi-Fi APs by a person in a moving vehicle, using a portable computer or PDA along with GPS and then optionally mapping these APs on a map. Wardriving originated from wardialing, a technique popularized by a character played by Matthew Broderick in a film WarGames [52]. There are many freely available types of software for wardriving on the Internet. These softwares are used to scan different wireless APs in the surrounding area. The most popular of these are Netstumbler [53] for Windows, Kismet [54] for Linux and Solaris, and KisMac [55] for Macintosh. There are different terminologies used in this context as given below:

**Warbiking** is the same as wardriving but instead of driving it involves searching of APs on a moving bicycle or motorcycle.

**Warwalking** (warjogging) is essentially the same as wardriving, except that it is done on foot rather than on a moving vehicle.

There are different projects like WIGLE [56] and Seattle’s Wi-Fi Map Project [57] and their aim is to collect information about Wi-Fi APs in different regions of the world. Then this information about the APs is plotted on maps. In December 2004, 100 students from undergraduate class set out to make a map of Seattle’s Wi-Fi network. Students were organized in groups with a laptop, Wi-Fi card and a GPS. They drove the Seattle Central neighborhoods scanning for Wi-Fi APs by using software called Netstumbler. This software recorded basic information about APs: AP name, secure or unsecure, commercial or free and the signal strength. All this information was recorded in a log file along with the latitude and longitude coordinates provided by the GPS device. A summary of the collected information is shown in the Table 5.1[57]. The Table shows that they found a total of 5225 APs; 52% AP were open (no WEP), 44% were secured with WEP encryption and 3% were pay-for-access. The logged information was plotted on maps e.g. as Figure 5.1[57].

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Number of APs</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP Enabled</td>
<td>2323</td>
<td>44</td>
</tr>
<tr>
<td>No WEP</td>
<td>2741</td>
<td>52</td>
</tr>
<tr>
<td>PAY</td>
<td>161</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>5225</td>
<td>100</td>
</tr>
</tbody>
</table>

The most popular web-based tool today is WIGLE (Wireless Geographic Logging Engine) [56]. The purpose of this project is to plot the recorded information about the APs on a map collected by users. On this web portal a registered user can upload the logged information about the APs along with GPS coordinates and then the APs are plotted on the map. According to the WIGLE, there are more than 20 million unique networks in the database, more than 1 billion unique locations, 48% of networks are secured (crypto), 34.3% networks are unsecured (no crypto) and 13.5% networks are with default SSID. This information is summarized in the Table 5.2 [56].

From the above given information, we can analyze that the Wi-Fi technology is very popular and huge number of APs have been deployed in many places like airports, shopping malls, cafeterias, railway stations etc. These Wi-Fi APs are installed by individual users, organizations, educational sectors and operators etc. Also we can observe that the art of wardriving is becoming very popular.
Individual users like to wardrive, collect APs information and plot it on a map which can be available for other people. By this exercise they can know the number of deployed APs in their region.

![Example Map of Wi-Fi in Seattle](image)

**Figure 5.1 - Example Map of Wi-Fi in Seattle**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique networks in the Database</td>
<td>20,472,402</td>
</tr>
<tr>
<td>Unique locations in the Database</td>
<td>1,076,554,696</td>
</tr>
<tr>
<td>Networks with crypto</td>
<td>9,807,237 (48%)</td>
</tr>
<tr>
<td>Networks without crypto</td>
<td>7,038,075 (34.3%)</td>
</tr>
<tr>
<td>Networks crypto unknown</td>
<td>3,627,090 (17.7%)</td>
</tr>
<tr>
<td>Networks with default SSID</td>
<td>2,762,626 (13.5%)</td>
</tr>
<tr>
<td>Registered Users</td>
<td>89,261</td>
</tr>
<tr>
<td>Files parsed</td>
<td>200,695</td>
</tr>
</tbody>
</table>

### 5.1 Methodology

In Paris, the Wi-Fi APs deployment is increasing exponentially. In many public places like railway stations, airports, hotels, shopping malls, cafeterias etc Wi-Fi APs have been installed. Therefore, we chose different sites in this city for our data collection and analysis. These sites include residential areas, shopping malls and skyscrapers for business industry. For our warwalking, we used a tablet PC.
with MS Windows XP operating system having Intel® PRO/Wireless 2200BG card along with an HTC TyTN II as a GPS device to log GPS coordinates. To scan Wi-Fi APs, we used Netstumbler [53] as warwalking tool. The limitation of this tool is that it does not provide the actual “Noise” value for many Wi-Fi cards. In our case, the noise value is 0. The GPS coordinates are actually the position of the mobile node where it received signals from an AP. It is not the actual position of an AP. We collected Wi-Fi logs at two different sites for different distances by warwalking in the streets. Site A is more residential and commercial area with congested and crowded population. Site B is more business and commercial area with skyscrapers. This site is wider and open and not very crowded. The warwalking track was completely natural as often followed by common people. We walked with normal pedestrian speed. At site A, we logged the Wi-Fi APs information for about 3.9 kilo meters and from site B for 4.5 kilometers in distance. The Wi-Fi information was captured for almost each second. The log includes AP SSID, MAC address, type, time, channel, SNR (signal to noise ratio), signal, noise and GPS coordinates (latitude and longitude). The warwalking tracks for site A and site B are shown in Figure 5.2 and 5.3 respectively.

![Figure 5.2 - Site A warwalking track](image)

### 5.2 Analysis

We collected a huge amount of Wi-Fi APs records along with the GPS coordinates from two sites in Paris. For data analysis, we considered the following assumptions:

- As a hypothesis, all the operators, public and private organizations and customers are willing to put their APs with open access. They have no encryption and require no credentials. This can be a realistic hypothesis, as some operators like FON give incentives to their customers who provide services to other users. Even an operator can deploy enough number of APs to cover the whole city.
We divided the whole warwalking track into 5 meters datasets. The purpose of this division is to make the analysis convenient, to draw a better picture of APs coverage and to deal with inaccuracy of GPS. The length of each dataset (5 meters) was just an assumption for this analysis.

In [58], it is explained that the SNR of an AP, measured at the MN, decreases as the range to MN increases. SNR directly impact the performance of a Wi-Fi connection. A higher SNR value means that the signal strength is stronger which allows higher data rates – overall offers better throughput. An SNR of 30dB may allow an IEEE 802.11g MN and AP to communicate at 24 Mbps. In [58], they performed extensive testing on Wi-Fi at various SNR values and concluded the following result.

- > 40dB SNR=Excellent (5 bars)
- 25dB to 40dB SNR=very good (3-4 bars)
- 15dB to 25dB SNR=low signal (2 bars)
- 10dB to 15dB SNR=very low signal (1 bar)
- < 10dB SNR=no signal

Therefore, in each dataset, we considered different threshold values for APs signal to noise ratio (SNR). For example, we took threshold values equal to 30dB SNR, 33dB SNR and 40dB SNR. The purpose of these threshold values is to check the possibility of best available signal for seamless mobility.

- All the APs are valid and legitimate. There is no fake AP.

From the collected Wi-Fi APs data, we want to figure out the following information:

- Average number of APs in each dataset
  As the whole warwalking track is divided into datasets, therefore we want to know the average number of APs in each dataset.

- Candidate APs
  It is a set of APs in each dataset with good signal strength and these APs are considered for handover. The purpose is to know that how many candidate APs are available for MN in each dataset. The process of selecting candidate APs is explained in next subsection.

- The number of APs seen for specific time duration
  The purpose is to find out the number of APs which are seen for long time duration (greater than 2 minutes) and these APs can be considered for association/connection if having good signal strength.

- Distribution of APs according to signal strength
  All the APs seen during data collection are distributed according to their signal strength. The purpose is to know the number of APs with good signal strength in each dataset.

- The coverage of APs deployed by different operators
  In Paris, different operators like FON, Orange etc have deployed enormous APs. With this analysis, we can find out the coverage area of individual operators.

- Channel utilization
  As the channel interference causes throughput degradation, therefore, we want to find out the statistics of channel utilization.
5.2.1 Access Points Statistics

We collected Wi-Fi APs records from two different sites; site A and site B. At site A, we encountered 1172 unique APs and site B 1015 APs. As we mentioned before that we divided warwalking track into datasets of 5 meters. In each dataset, we have several records for each unique AP and may have different signal strength values. For optimal solution, from each dataset we took that record for each unique AP which has the lowest signal strength value. It means that we selected each unique AP with weakest signal strength for optimality. Then from this set of records with lowest signal strength for each unique AP, we considered the one unique AP record with highest signal strength value. So from each dataset, we considered one unique AP with highest of lowest signal strength value. The purpose of this method is to have an optimal solution with respect to signal strength of APs. Table 5.3, shows the statistics of APs gathered from site A. The table illustrates minimum and maximum SNR values in all datasets. In the table, column “Drop of Signal” means that in how many datasets we would not be able to continue the service or have seamless mobility. The value in the column shows the number of occurrences and percentage of drop of signal. At site A, if we take SNR value of 30dB then we have only 0.88% of area where we have no Wi-Fi coverage and for 99.12% of area we have Wi-Fi coverage. Now considering the SNR value of 33dB, we have 96.74% Wi-Fi coverage and only for 3.26% of area there is no Wi-Fi coverage. It means that if we want to keep the stronger signal strength as a threshold then we will have a bit less coverage. That is why for signal strength of 30dB, the Wi-Fi coverage is 99.12% while for 33dB the Wi-Fi coverage is 96.74%. Still with better signal strength, there is enough Wi-Fi coverage to offer seamless mobility services. From all the datasets, we also calculated the average number of APs. From Table 5.3 in column 5, we observe that if the threshold value of signal strength is low (weak signal strength) then we have more average number of APs in each dataset i.e. for SNR=min the average number of APs is 34.94, for SNR>=30 the number is 14.65, for SNR>=33 the number is 7.8 and for SNR>=40 the number is only 1.4. These average numbers of APs in each dataset are then distributed according to signal strength which is shown in Table 5.3. We distributed the SNR in four portions; 15-30, 30-40, 40-50 and 50-60. At site A, for threshold value of SNR=min, the average number of APs in each dataset is 34.94. This average number of APs is then divided according to the signal strength. For the range 15<=SNR<=30 the
average number of APs are 22.76, for range 30<=SNR<40 the average number of APs are 11.75, for range 40<=SNR<50 the average number of APs are 0.44 and for range 50<=SNR<60 the average number of APs in each data set are 0.006. This distribution shows that for the same threshold value of signal strength, in the average number of APs in each dataset most of the APs have weak signal strength and very few APs have stronger signal strength. For seamless mobility there should be enough APs in each dataset to perform handover and continue the services. This distribution can cooperate in determining the possibilities for seamless mobility in such environments. Similar statistics of APs from site B are elaborated in Table 5.4.

Table 5.3 - Access points statistics from site A

<table>
<thead>
<tr>
<th>SITE A</th>
<th>Min SNR</th>
<th>Max SNR</th>
<th>Drop of Signal (number &amp; %)</th>
<th>Avg no. of APs/dataset</th>
<th>15&lt;=SNR&lt;30</th>
<th>30&lt;=SNR&lt;40</th>
<th>40&lt;=SNR&lt;50</th>
<th>50&lt;=SNR&lt;60</th>
</tr>
</thead>
<tbody>
<tr>
<td>APs with SNR=min</td>
<td>17</td>
<td>56</td>
<td>none</td>
<td>34.94</td>
<td>22.76</td>
<td>11.75</td>
<td>0.44</td>
<td>0.006</td>
</tr>
<tr>
<td>APs with SNR&gt;=30</td>
<td>30</td>
<td>56</td>
<td>1 (0.88%)</td>
<td>14.65</td>
<td>-</td>
<td>14.2</td>
<td>0.448</td>
<td>0.006</td>
</tr>
<tr>
<td>APs with SNR&gt;=33</td>
<td>33</td>
<td>56</td>
<td>8 (3.26%)</td>
<td>7.8</td>
<td>-</td>
<td>7.36</td>
<td>0.48</td>
<td>0.006</td>
</tr>
<tr>
<td>APs with SNR&gt;=40</td>
<td>40</td>
<td>56</td>
<td>Many</td>
<td>1.4</td>
<td>-</td>
<td>0</td>
<td>1.39</td>
<td>0.01</td>
</tr>
</tbody>
</table>

In Figure 5.4 the APs with the threshold values of SNR=min and SNR>=30dB are demonstrated for each dataset in site A. The graph shows the records with SNR=min and SNR=30dB. Here the line with SNR=min is overlapped by the line with SNR>=30dB except for few datasets where there is no Wi-Fi coverage if we consider the threshold value of 30dB. We can observe from the graph that in most of the datasets the APs have good quality of signal for both threshold values (SNR min and 30dB). Throughout the track we are able to have Wi-Fi coverage. But for SNR=min in few datasets the SNR value is as low as 26 dB and we can observe one drop of signal (means no Wi-Fi coverage) in few datasets continuously for SNR>=30 which is 0.88% of the total Wi-Fi coverage. In these locations we would not be able to achieve seamless mobility. As mentioned before ‘drop of signal’ means that in a particular dataset we do not have any AP with SNR value 30dB or greater. But for rest of the datasets (means 99.12%), we have good quality of signal. To better analyze the quality of signal for this track, now we compare two different threshold values SNR=min and SNR>=33dB. By these thresholds, we assume that for each dataset the APs SNR must be minimum and 33dB or above. We want to investigate the Wi-Fi coverage if we consider better quality of signal strength APs (threshold of SNR>=33) in each dataset. The results of these thresholds are depicted in Figure 5.5.

Table 5.4 - Access points statistics from site B

<table>
<thead>
<tr>
<th>SITE B</th>
<th>Min SNR</th>
<th>Max SNR</th>
<th>Drop of Signal (number &amp; %)</th>
<th>Avg no. of APs/dataset</th>
<th>20&lt;=SNR&lt;30</th>
<th>30&lt;=SNR&lt;40</th>
<th>40&lt;=SNR&lt;50</th>
<th>50&lt;=SNR&lt;60</th>
</tr>
</thead>
<tbody>
<tr>
<td>APs with SNR=min</td>
<td>18</td>
<td>58</td>
<td>none</td>
<td>33.5</td>
<td>25.83</td>
<td>7.4</td>
<td>0.232</td>
<td>0.006</td>
</tr>
<tr>
<td>APs with SNR&gt;=30</td>
<td>30</td>
<td>58</td>
<td>2 (0.21 %)</td>
<td>9.5</td>
<td>-</td>
<td>9.23</td>
<td>0.242</td>
<td>0.007</td>
</tr>
<tr>
<td>APs with SNR&gt;=33</td>
<td>33</td>
<td>58</td>
<td>24 (13.2 %)</td>
<td>4.4</td>
<td>-</td>
<td>4.1</td>
<td>0.287</td>
<td>0.008</td>
</tr>
<tr>
<td>APs with SNR&gt;=40</td>
<td>40</td>
<td>58</td>
<td>Many</td>
<td>0.707</td>
<td>-</td>
<td>0</td>
<td>0.696</td>
<td>0.012</td>
</tr>
</tbody>
</table>
We observed several numbers of drops of signal in some datasets for \( \text{SNR} > 33 \text{dB} \). In these locations, there is no Wi-Fi coverage and we cannot achieve continue services. But if we compare it to all Wi-Fi records track, about 2% there is no Wi-Fi coverage and 98% we have coverage with minimum SNR value equals to 33dB which is quite enough for offering seamless mobility to end users. Now we assumed threshold value of \( \text{SNR} \geq 40 \text{dB} \) and we observed many numbers of drops in the each
dataset. Most of the time, we do not have Wi-Fi coverage and it is impossible to offer seamless services in this situation.

The above mentioned analysis and observations were carried out on data collected from site A. Similar methods and techniques were applied on data collected from site B. We want to determine the Wi-Fi coverage with certain threshold values for SNR on site B. Figure 5.6 depicts the results obtained when we considered the threshold SNR=min and SNR>=30dB. In the graph considering SNR=min, we can observe that throughout the warwalking path, we have Wi-Fi coverage or signals. But in some datasets, we have very low SNR values which are not sufficient for some high bandwidth and delay sensitive applications. For this reason, we considered the threshold value of SNR>=30. We can observe from the graph that we have good coverage of Wi-Fi APs and can offer better services except for few datasets where there is a drop of signal. Therefore, we can say that it is possible to offer seamless mobility in this situation with regard to Wi-Fi coverage and better signal strength.

Now we compare the threshold SNR values of minimum and >=33dB. For SNR>=33dB, we observed that there are many datasets where we do not have Wi-Fi coverage and seamless mobility is not possible in this case. These results are shown in Figure 5.5A (see Appendix A). Next we considered the threshold SNR=min and SNR>=40dB. For SNR>=40dB, we observed that there were also many datasets with no Wi-Fi coverage and it is not possible to offer seamless mobility in this situation as well.

![APs Coverage Graph with SNR=min, 30](image)

**Figure 5.6 - Site B APs coverage with SNR=min and SNR>=30dB**

### 5.2.2 Candidate APs

In this section we want to observe the number of candidate APs for handover in each dataset. Candidate APs are those APs which are considered for handover in next dataset. For this analysis, we checked the SNR values of all the records of each AP in dataset. Then considered the APs in the dataset, which SNR values are increasing (signal strength is getting better) and these APs have an SNR value greater than a certain threshold in the dataset $i$. It shows that the signal strength of these APs is getting better in dataset, and still they have good quality of signal strength (above a certain threshold value) in dataset $i+1$. For example, in Figure 5.7, there are two datasets i.e. dataset, and dataset $i+1$. In the Figure, x-axis shows the number of scans in each dataset and y-axis shows the SNR value for each AP. Each dataset has two scans means that in each dataset we received two signal packets showing the SNR values for each AP. There are total 5 APs (AP1-AP5). In scan1 and scan2,
the SNR values of AP1 are 25dB and 32dB respectively. In dataset, the SNR values of AP1 are increasing. We can assume that MN is getting closer to the AP1. By considering the AP1 in dataset, now we check that the SNR value of AP1 in dataset$_{i+1}$ is greater than a threshold value (i.e. 30dB). As its SNR value in scan3 of dataset$_i$, it is 28dB which is less than threshold value of 30dB. So we cannot choose AP1 as a candidate AP. Now considering AP2 in scan1 and scan2 of dataset$_i$, its SNR values are 28dB and 30dB. In scan3 and scan4 of dataset$_{i+1}$, its values are 33dB and 35dB which are above than the threshold value of 30dB. Therefore, we select AP2 as a candidate AP. Similarly AP4 is also a candidate AP according to our mentioned rules. So the MN can perform handover to one of these APs. We call such APs as candidate APs. The results of such analysis are shown in Figure 5.8. In this analysis, we considered the threshold values of SNR>=30 and SNR>=33. In the graph the line with SNR>=30 shows the number of candidate APs with threshold value of SNR=30 or greater and the line with SNR>=33 shows the number of candidate APs with threshold value of SNR=33 or greater. Therefore, we select AP2 as a candidate AP. Similarly AP4 is also a candidate AP according to our mentioned rules. So the MN can perform handover to one of these APs. We call such APs as candidate APs. The results of such analysis are shown in Figure 5.8. In this analysis, we considered the threshold values of SNR>=30 and SNR>=33. In the graph the line with SNR>=30 shows the number of candidate APs with threshold value of SNR=30 or greater and the line with SNR>=33 shows the number of candidate APs with threshold value of SNR=33 or greater. The graph elaborates the number of candidate APs for handover in the next dataset. For threshold value of SNR>=30, there are enough candidate APs in each dataset to perform handover. For threshold value of SNR>=33, in some datasets there are no candidate APs which means that we cannot perform handover in this dataset and the MN has to be in communication via old AP. If we compare the two lines, we can observe that there are less number of candidate APs available in each dataset of SNR>=33 than SNR>=30. The reason is obvious that in former case the signal strength of APs is stronger than in later one. This means that we want to check the possible number of candidate APs in the next dataset which SNR value is greater than 33. So in many cases we do not have Wi-Fi coverage and it is impossible to offer seamless mobility in this situation.

Now we want to calculate the number of candidate APs for handover in datasets collected from site B. As we mentioned earlier that by candidate APs we mean that those APs in a given dataset which SNR value is increasing and for those APs the SNR value is greater than a certain threshold SNR value in next dataset. Figure 5.8A (see Appendix A) shows the results of candidate APs in each data set when we consider the threshold SNR values of 30dB and 33dB. It depicts a reasonable number of candidate APs in next dataset if we consider the threshold value of SNR>=30. It means that we have enough number of candidate APs to perform handover and can achieve our goal of seamless mobility.
But for the threshold SNR>=33, we can observe from the graph that there are less number of candidate APs for handover in next dataset as compared to SNR>=30. The reason is obvious that in former case, the signal strength of APs is stronger than in later one. Therefore, it seems a bit difficult to perform handover in few datasets and offer seamless mobility. The summary of candidate APs for all threshold values in site A and B is shown in Table 5.5. This table shows the average number of candidate APs with threshold SNR values of 30dB and 33dB for site A and B. By comparing the two sites, we can observe high average number of candidate APs with threshold SNR values of 30dB and 33dB for site A than site B. The reason could be that site A is more residential and shopping area with high density population. While site B is more business and commercial area with skyscrapers. Site B is more wide and open area while site A is more crowded and congested area. These results and observations can be very useful for determining the possibilities of fast handover and seamless mobility in such environments. From the above statistics and analysis, we can conclude that there is a possibility for seamless mobility in the two mentioned sites. From the Table 5.5, if we consider the SNR value of 30 for site A, we have an average of 9.53 candidate APs. For site B, we have 6.14 average candidate APs in each dataset. Both these average values indicate suitable number for candidate APs. Similarly observing the SNR value of 33dB from Table 5.5 for site A, we have an average of 4.15 candidate APs in each dataset which is also a suitable value for candidate APs. Considering the same SNR value for site B, we have an average of 2.25 candidate APs in each dataset. It means that in this case we have at least 1 AP as a backup. Assume if one AP is down, still we have another one AP to perform handover to. This situation is very strict in sense that we have only 2 candidate APs in each set to perform handover as compared to previous case. Similarly for site B, we can consider the threshold SNR value of 30. This summary shows us that we have reasonable number of candidate APs with enough signal strength to perform handover and offer seamless mobility to the valued customers.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Site B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average number of candidate APs with SNR&gt;=30</td>
<td>9.53</td>
</tr>
<tr>
<td>Average number of candidate APs with SNR&gt;=33</td>
<td>4.15</td>
</tr>
</tbody>
</table>

Table 5.5 - Summary of candidate APs
5.2.3 APs Deployed by Operators

In Paris the Wi-Fi services are offered by different operators like Freewifi, Neuf, and Orange etc. These are some big players in the market nowadays. From our warwalking data, we also computed Wi-Fi coverage of different operators. The purpose of this analysis is to find out the Wi-Fi coverage of individual operator in the city and to know that is there any operator which provides enough Wi-Fi coverage to offer seamless services. From our results in Table 5.6, we observed that there is not a single operator which provides full Wi-Fi coverage in urban environment of Paris. All the operators offer about 72% of Wi-Fi coverage which is not sufficient for seamless mobility. There are two possibilities to cope with this problem. First, an operator should deploy enough APs in order to provide Wi-Fi coverage. This solution is valuable if the operator has enough budgets to buy and deploy APs. Also there are reasonable number of customers of this operator for whom to deploy the infrastructure and offer the services. Second, different operators should collaborate with each other and provide ubiquitous services to their valued customers. This solution is reasonable but depends on the agreement between the operators and the services they offer to their customers.

<table>
<thead>
<tr>
<th>Operators</th>
<th>Wi-Fi Coverage in %</th>
<th>No Wi-Fi Coverage in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeWiFi</td>
<td>73</td>
<td>27</td>
</tr>
<tr>
<td>Neuf</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>freephonie</td>
<td>73</td>
<td>27</td>
</tr>
<tr>
<td>Livebox</td>
<td>71</td>
<td>29</td>
</tr>
</tbody>
</table>

Table 5.6 - Wi-Fi coverage by operators with SNR>=30dB

5.2.4 Channels Utilization

It is also very important to know about the channel utilization of different Wi-Fi networks. If the neighboring APs are using the same channel number then it can cause interference to each other and can affect the throughput along with quality of service. From the dataset we also computed the percentage (%) of channel utilization in each dataset. Table 5.7 illustrates the average channel utilization and average maximum channel utilization in all the dataset. It depicts that channel 1, 6 and 11 are mostly used i.e. channel 1 for 24%, channel 6 for 13.85% and channel 11 for 28.36%. Also in the Table 5.7 row number 3 shows the maximum average utilization for each channel. The values for channel 1, 6 and 11 are 46.34%, 40% and 58.82% respectively. We observed that most of the APs were using channel numbers 1, 6 and 11. The reason for this high utilization is that these three channels are non-overlapping channels in Wi-Fi technology and sometime these channels are configured by default. Most of the users do not know about this terminology. They leave the default setting on the APs. But with better deployment and management, we can achieve the best performance.

<table>
<thead>
<tr>
<th>Channel#</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg. %</td>
<td>24.06</td>
<td>4.54</td>
<td>0.83</td>
<td>1.81</td>
<td>2.82</td>
<td>13.85</td>
<td>4.72</td>
<td>3.71</td>
<td>3.32</td>
<td>7.29</td>
<td>28.36</td>
<td>2.05</td>
<td>2.64</td>
</tr>
<tr>
<td>Max. %</td>
<td>46.34</td>
<td>50</td>
<td>5.88</td>
<td>16.67</td>
<td>14.71</td>
<td>40</td>
<td>15.69</td>
<td>21.05</td>
<td>20</td>
<td>20.59</td>
<td>58.82</td>
<td>24.14</td>
<td>23.08</td>
</tr>
</tbody>
</table>
5.2.5 APs Seen for Specific Time Duration

It is very important to find out the time duration for which an AP is seen. There can be the possibility that an AP was seen with strong signal strength but for very short time. Then it is not possible to perform handover to this AP because of the short time duration. In such situation, a MN has to perform handovers very frequently. It is valuable to perform handover to an AP which has a longer life and with this mechanism we can optimize the solution by minimizing the number of handovers. Figure 5.9 demonstrates the number of APs seen for specific time duration in the data collected from site A. In the graph the first value 160 are the total number of APs seen for time duration between 0 and 1 minute. It means that in all datasets there were 160 APs which were seen for this time. These APs are irrelevant of their position in the datasets. Similarly if we consider the second value 63, it means that these 63 APs are seen for time duration between 1 and 2 minutes. Now here this value excludes the APs which were seen for time duration between 0 and 1 minute. If we want to find out that how many APs were seen for time duration of less than or equal to 2 minutes then the result will be 160+63=223. The graph shows that most of the APs were seen for the time duration between 2 and 3 minutes which are 550 in numbers. If we want to find out that how many APs were seen for time less than or equal to 3 minutes then the result will be 160+63+550=773. The same analysis is done for the data collected from site B and is shown in Figure 5.9A (see Appendix A). By comparing the two Figure 5.9 and 5.9A, we can see that both the figures are correlated. These figures show similar results in term of the time duration for which an AP is seen. From these figures we can conclude that there are many APs which are seen for long time duration and are well enough to perform handover.

![Figure 5.9 - Number of APs seen for specific time duration at site A](image)

In previous paragraph we found the number of APs seen for specific time duration and most of the APs are seen for reasonable long time but we don’t know the signal strength of these APs. For example it is very important to know the signal strength of the APs seen for time duration between 2 and 3 minutes. We showed that most of the APs from both sites A and B are seen for this time duration. This time duration of an AP is quite good to be considered for handover but it is very important to know its signal strength. It is not efficient to perform handover to an AP which is seen for long time but with weak signal strength and it will not be able to provide good quality of service with seamless mobility. Now we want to find out the signal strength distribution of these APs found for the specific time duration. The Figure 5.10 illustrates the results for signal strength distribution according to APs seen for specific time duration at site A. From the figure we can observe that the APs seen for time duration between 0 and 1 minute (160 APs) are distributed in 0 AP with SNR=60dB, 1 AP with SNR=50dB, 16 APs with SNR=40dB, 60 APs with SNR=30dB and 83 APs with SNR=20dB i.e. 0+1+16+60+83=160. Similarly we can see the same signal strength distribution for other APs as well. From these results we can say that most of the APs have weak signal strength and are not suitable to perform handover to these APs. From the figure we can analyze that very few APs
have the best signal strength. But still there are enough numbers of APs with good signal strength which are seen for reasonable long time duration. The same analysis are carried out on the data collected from site B and the results are shown in Figure 5.10A (see Appendix A)

![Figure 5.10 - Number of APs with SNR distribution at site A](image)
Evaluation

In this project, we analyzed the deployment of Wi-Fi APs in Paris city. We conducted data collection by warwalking at two (2) locations. To find Wi-Fi coverage, we considered some threshold values for better quality of signal. Even with SNR value of 30dB and greater, there is 99% of Wi-Fi coverage both at site A and site B. It means that there is enough Wi-Fi coverage to offer seamless services. We computed the average number of APs in each dataset. With SNR value of 30dB and greater, there were 15 average number of APs at site A and 10 APs at site B. We also calculated the average number of candidate APs in each dataset. There were 10 average number of candidate APs in each dataset with SNR=>30dB at site A and 6 average number of candidate APs with SNR=>30dB at site B. It illustrates that there are enough candidate APs to be considered for handover in each dataset. Most of the APs at both sites were seen for more than 3 minutes of time duration. We consider this time duration suitable for handover scenarios. Based on our assumptions, analysis, measurements and results mentioned above, we conclude that there is a possibility for seamless mobility in such environment.
Conclusion

In Paris the Wi-Fi APs have been deployed enormously because the Wi-Fi technology is cheap, provides high bandwidth, and can be deployed and maintained easily. The motivation of the project was to know the real status of the deployed APs in this city, average number of APs in each dataset, number of candidate APs for handover, distribution of APs according to signal strength, coverage of APs deployed by different operators, channel utilization and check the possibility for seamless mobility especially for VoIP over Wi-Fi networks. Also the customers, who have subscribed with the operators, can reutilize the resources deployed by their operators in the urban areas. There is no such kind of work done before. Therefore, we collected Wi-Fi APs information at two sites A and B. Site A is more residential and commercial area with congested and crowded population. Site B is more business and commercial area with skyscrapers. This site is wider and open and not very crowded. The warwalking track was completely natural as often followed by common people. We walked with normal pedestrian speed. At site A, we logged the Wi-Fi APs information for about 3.9 kilo meters and at site B for 4.5 kilometers in distance. The Wi-Fi information was captured for almost each second. The log includes AP SSID, MAC address, type, time, channel, SNR (signal to noise ratio), signal, noise and GPS coordinates (latitude and longitude).

From our analysis we made some assumptions i.e. as a hypothesis, all the operators, public and private organizations and customers are willing to put their APs with open access (no credentials), the warwalking track is divided into 5 meters of datasets, different threshold values for APs signal to noise ratio, all the APs are valid and legitimate (no fake AP).

From our analysis and results, we came to know that there is enough Wi-Fi coverage with good signal strength. In each dataset, there are reasonable numbers of candidate APs available to perform handover. We computed the time duration for which each AP was detected. We noticed that most of the APs were seen for the time duration between 2 and 3 minutes. We can assume that it is reasonable time to consider an AP for handover. We also figured out the signal strength of these APs and found that quite good number of APs have strong signals. In Wi-Fi networks, channel utilization plays an important role in throughput. If overlapping channels are used then it will cause interference and will affect the throughput of the network. From our collected data, we observed that most of the networks were using non-overlapping channels (1, 6 and 11). The reason could be that these channels are configured by manufacturers as default and most of the individual users don’t know about this terminology. The enormous amount of Wi-Fi APs in Paris city is due to some big players like Orange, FON, etc in the market. We want to know the status of individual operators deployed APs. Our results illustrates that each operator offers about 72% of APs coverage in the area where we did warwalking. We suggested two possibilities to offer full Wi-Fi APs coverage: a) An operator should deploy enough APs or b) different operators should collaborate with each other.

In this project, we used the SSS (Strongest Signal Strength) algorithm for the selection of an AP which is a simple and easy to deploy algorithm. It means that we did not consider the total capacity, the offered bandwidth, load, delay and throughput of an AP. But from our results we can observe that we have enough number of candidate APs, so we can handover from one AP to another easily. If we want to consider these parameters, then the operators have to deploy a very complex architecture of 802.21 (MIH) which can assist the MN in selecting the best AP among several candidate APs. This architecture will be very useful in situation when we want to perform a vertical handover (Wi-Fi to WiMAX or Wi-Fi to GSM etc).

Finally we concluded that based on our assumptions, collected information, analysis, observations and results there is a possibility to offer seamless mobility services to the customers in the Paris city.
Future Work

This project is in the beginning phase. It has a vast field of work to be considered in future. In this project, we collected Wi-Fi APs information at two sites. For more accurate analysis it would be better to collect this information for more than 6 sites and then analyze the data and compare the results. At each site collect several sets of data during different time of the day. These sites should include residential, business, commercial and tourist places. By many samples of data, we can model this work in more efficient way. We logged the Wi-Fi APs information only by warwalking. The same information can also be collected by warcycling and wardriving. Then compare the results with warwalking. The speed with which the information is collected is very crucial. The information will be collected at different speeds (warwalking, warcycling and wardriving) which can affect the analysis.

In future if there is enough Wi-Fi APs coverage provided by a single operator or there is collaboration between different operators, real tests of seamless mobility should be performed in order to observe the services like VoIP. Then we can also consider the quality of service, delay and security issues. Finally, we would like to consider vertical handover or heterogeneous technology handover (Wi-Fi to Wimax and Wi-Fi to GSM etc) in the future work and observe the seamless mobility of real time and delay sensitive applications like VoIP.
References

IP Mobility Support for IPv4, RFC 3344, August 2002.
Moon Kim, et al., “A Study on IEEE 802.21 MIH Frameworks in Heterogeneous Wireless Networks”, Dept. of Inform. & Telecom. Eng., Graduate School of Korea Aerospace University.

APPENDIX A

Figure 5.8A - Site B APs coverage with SNR=min and SNR>=33dB

Figure 5.9A - Number of APs seen for specific time duration at site B
Figure 5.10A - Number of APs with SNR distribution at site B