WiFi-WhiteFi Handover: Signaling and Performance

Budoor Saeed Abdullah Bawazeer

A thesis submitted for the requirements of the degree of Master of Computer Science

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY
KING ABDULAZIZ UNIVERSITY
JEDDAH – SAUDI ARABIA

Rabe' II, 1436H- February, 2015G

بسم الله الرحمن الرحيم

قال تعالى ﴿ وَمَا تَوْفِيقِي إِلا بِاللهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ ﴾
سورة هود آية ٨٨

WiFi-WhiteFi Handover: Signaling and Performance

By Budoor Saeed Abdullah Bawazeer

A thesis submitted for the requirements of the degree of Master of Computer Science

Supervised By

Dr.Ghada Al-Dabbagh
Dr.Nadine Akkari

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY
KING ABDULAZIZ UNIVERSITY
JEDDAH – SAUDI ARABIA

Rabe' II 1436H- February 2015G

Dedicated to

My family

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Merciful, the Most Compassionate, all praise be to Allah, the Lord of the Worlds, and prayers and peace be upon Mohamed, His servant and messenger.

First and foremost, I must acknowledge my limitless thanks to Allah, the Ever-Magnificent, the Ever-Thankful, for His help and blessing. I am sure that this work would have never been completed without His guidance.

I am grateful to the people who worked hard with me from the beginning to the completion of this present research, particularly my supervisors, **Dr. Ghadah AlDabbagh** and **Dr. Nadine Akkari**, for their efforts, motivation, encouragement, and continuous support. It was an honor for me to work with them. Also, I would like to thank **Dr. Nikos Dimitriou** for his support and guidance. Finally, I would like to thank my boss **Dr. Mai Fadel** for being patient with me throughout the research period.

I would also like to express my wholehearted thanks to my family (**my father, mother, husband, sisters, and sons**) for the generous support they have provided me throughout my entire life and particularly throughout my Master's degree. Because of their unconditional love and prayers, I have had the chance to complete this thesis.

WiFi-WhiteFi Handover: Signaling and Performance

Budoor Saeed Abdullah Bawazeer

Abstract

Today, wireless networks are becoming increasingly important due to the widespread use of smartphones. To achieve Always Best Connectivity (ABC), mobile nodes (MNs) should change their access points (APs) when they need to retain Quality of Service (QoS). Integration between networks will help the MN to perform handover (HO) from one network to another. HO is the process of changing the point of attachment. IEEE 802.21 is a protocol to unify this process independently, irrespective of the type of the two networks involved. TV white space (TVWS) is an unused license radio spectrum that provides superior propagation and building penetration compared to other spectrums. TV band primary users (PUs) occupy the channels for a certain time, meaning that the availability of WS spectrums in a given location can vary with time. The United States Federal Communications Commission (FCC) determines the range of channels to be used by secondary (unlicensed) users (SUs) when not being used by a PU. IEEE 802.11af (WhiteFi) is a new standard, which is an amendment to the MAC/PHY layers of IEEE 802.11 that allows WiFi to use the TVWS spectrum. WhiteFi can be used to fill the gaps between WiFi networks due its extensive area of coverage. HO to WhiteFi networks will give users a low cost choice. Therefore, this work studies the HO between WiFi and WhiteFi networks. In IEEE 802.11 networks, the scanning process to discover the neighbor networks causes a major delay in the HO. Scanning process can perform in a passive way where MN should wait 100 ms on each channel to receive a potential beacons come from APs, or in active way where MN doesn't wait; instead it sends request on each channel then collects responses. In general, active scan spend less time than passive method specially on the channels where no AP is there. In WhiteFi, the scanning time will increase due to the increased number of TVWS channels compared to normal WiFi and to the rule which force to passively scan these channels. Using IEEE 802.21 protocol, this work proposes two solutions to reduce scanning time. First, "Scan free," in which the MN obtains a schedule for local TVWS by querying an information server (IS), which updates every 48 h. Second, "Scan active," in which the MN queries the IS to retrieve the current active channels currently used by APs from the registered location secure server (RLSS), the local server of WhiteFi, so the MN will scan fewer channels and thus decrease the total delay. The performance of these two schemes is evaluated using an analytical model and compared to the base case "Scan all" in which all channels are scanned. The results show that scanning only active channels will reduce the scan delay, while the risk of changing network conditions will not affect the delay if the number of active channels is reduced. Scan free is the most stable scheme but it may waste time by scanning empty channels.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND TERMINOLOGY

Symbol	Definition
AP	Access Point
BSS	Basic Service Set
BU/BAck	Bind Update/Acknowledgment
CoA	Care of Address
CR	Cognitive Radio
DAD	Duplicate Address Detection
ESS	Extended Service Set
FBU/FBAck	Fast Bind Update/ Acknowledgment
FCC	Federal Communications Commission
FMIP	Fast MIP
FNA	Fast Neighbor Advertisement
GDB	Geolocation Database
GDD	Geolocation Database Dependent
HA/FA	Home/Foreign Agent
HHO	Horizontal Handover
HI/HAck	Handover Initiation/Acknowledgment
HMOP	Hierarchical MIP
HO	Handover
IEs	information elements
IS	Information Server
ISM	Industrial, Scientific, Medical
LCoA/ RCoA	on-Link CoA /Regional CoA
LGD	Link_Going_Down
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MAP	Mobility Anchor Point
MD	Movement Detection
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MIP	Mobile IP
MN	Mobile Node
NAR/PAR	New/Previous Access Router

NAP/PAP	New/Previous Access Point
Ofcom	Office of Communications
PMIP	Proxy MIP
PU	Primary User
QoS	Quality of Service
RLQP	Registered Location Query Protocol
RLSS	Registered Location Secure Server
RSS	Receive Signal Strength
RtSolPr/ PrRtAdv	outer Solicitation for Proxy Advertisement/Proxy Router Advertisement
SAP	service access point
SAPs	Service Access Points
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
SU	Secondary User
TVWS	TV White Space
UMTS	Universal Mobile Telecommunications System
VHO	Vertical Handover
WiFi	wireless fidelity
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WRAN	Wireless Regional Area Network
WSM	White Space Map
WSP	Wireless Service Provider

Chapter 1

Introduction

1.1 Introduction

Nowadays, with the increasing number of smart devices and handheld computers, people want to send and receive data and connect to others from anywhere, at any time. Therefore, mobile devices must always be connected when moving across homogeneous or heterogeneous networks. This is achieved by enabling the mobile device to detect all networks in its range and select one of them to perform a seamless handover (HO) to it. Thus, the HO is the most important process when considering network integration.

Millions of wireless adapters follow the IEEE 802.11 standard (a type of Wireless Local Area Network (WLAN)). Many laptops come with IEEE 802.11b, 802.11g, or 802.11n (WLAN) adapters integrated this is because the 2.4 GHz is available worldwide as unlicensed band [1]. All WLANs suffer from limitations, for example IEEE 802.11a and IEEE 802.11b networks cannot cover more than 300 meters, even in ideal conditions [2]. Therefore, users connected to WiFi must connect to another network when they leave its range to maintain internet service. Several studies [3-5] considered the integration between WiFi with other networks such as 3G and WiMAX in order to keep connectivity.

One of the criteria for choosing the network to perform the HO is the access cost. The “TV” band is an appropriate choice due to its extended coverage capabilities and its availability following the analog-digital TV switchover. The United States Federal Communications Commission (FCC) named the unused TV spectrum "White Spaces". TV White Space (TVWS) is an unused TV spectrum with a lower frequency than WiFi but with a higher bandwidth. In addition to its low cost, the relatively lower frequency require low power designs compared to those at higher frequencies [6].

The idea of using TV bands to transfer data first appeared when digital transmission was introduced in TV broadcasting, resulting in more efficient spectrum usage and unused portions of the TV band that were previously used for analog transmission. These bands have many advantages, since they can allow the use of higher signal bandwidths and the transmitted wireless signals can penetrate surfaces and walls. Therefore, their propagation range can be extended up to 100 km. The FCC has divided the band into 51 channels and prevented unlicensed operation on four of those channels. In addition, the FCC allows only fixed devices to operate on 17 channels, and the remaining 30 channels allow for all type of devices, including portable devices [7]. The first standard developed in this area was IEEE 802.22. IEEE recently developed a new standard that uses TVWS bands by modifying the two layers (physical and medium) of the traditional WiFi. This standard is called IEEE 802.11af, and since it is a WiFi amendment using TVWS, it is known as

"WhiteFi." It may be used to fill the gaps between WiFi networks, enabling a user to maintain connectivity after leaving a regular WiFi hotspot (Figure 1).

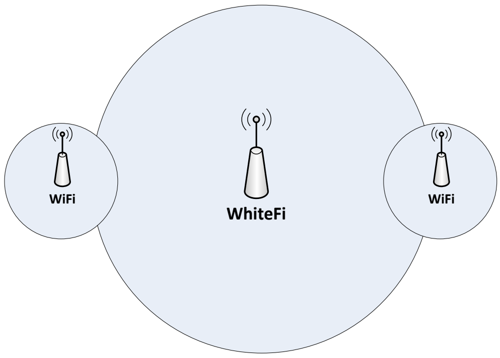

Figure 1. WhiteFi covers the gaps between WiFi networks

To support a seamless HO between heterogeneous networks, the Institute of Electrical and Electronic Engineers (IEEE) produced the IEEE 802.21 standard. IEEE 802.21 [8] is a new standard that aims to make a uniform protocol for HO between IEEE 802 and non-IEEE 802 networks, known as Media Independent Handover protocol (MIH). MIH applies a cross-layer design, which allows one layer to interact with another and exchange information. IEEE 802.21 consists of a framework that enables service continuity while a mobile node (MN) transitions between heterogeneous link-layer technologies. The MIH helps the decision phase of the HO by gathering information about neighboring networks and preparing for the HO.

The MIH is not involved in the execution of the HO itself except to give commands to the interfaces to establish a media access control (MAC) layer (L2) HO, which is link layer dependent. A network layer (L3) HO should be executed to help manage the IP address when an MN changes its location. Protocols such as MIPv4 and MIPv6 are used in L3 HO for this purpose. FMIPv6 is an enhanced version of MIPv6 protocol which reduces the period that MNs cannot receive or transmit data in the

HO process. This is done by starting the preparation of L3 HO before L2 HO commences.

In our research, we aim to find an efficient mechanism to use in the HO process between WiFi and WhiteFi and study its performance in term of HO delay.

1.2 Motivation

WhiteFi has large coverage due to the propagation properties of the TV band. One use of TVWS networks is to fill the gaps between small networks such as WiFi hotspots. When a user moves between WiFi/WhiteFi, the HO mechanism is needed. Because no previous work exists regarding the HO from/to WhiteFi networks, our research focuses on studying the HO delay from WiFi to WhiteFi.

1.3 Problem Statement

IEEE 802.11af (WhiteFi) is a new standard from IEEE 802.11. Amendments apply to L1 and L2 (MAC/PHY layers) of IEEE 802.11 that allow IEEE 802.11af to use the TV band. Because FCC allows portable devices to operate only on 30 TV channels, MN needs to scan channels more than normal WiFi with 11 channels when it needs to connect to WhiteFi networks. For WiFi networks, the scanning time causes most of the HO delay, and this may lead to HO failures due to the possible loss of coverage from the WiFi network before finishing the scanning procedure and the following steps for registering with a WhiteFi network. In IEEE 802.11, MN can scan channels in passive or active way. Passive scan is where MN spend 100 ms on each channel waiting for beacons sending by APs regardless of the existence of them or not. In active scan, MN doesn’t wait for beacons. Instead, MN sends a request on a channel then collects the responses if any and moving to the next spending less time than passive process specially when no AP exist. Scanning delay in WhiteFi will take long time not only because of number of channels but due to FCC rules that prevent active scanning method which take less than passive method which is allowed by FCC. Our research focuses on designing a new mechanisms to reduce the delay of scanning process of HO from WiFi to WhiteFi networks.

1.4 Thesis Objectives

The proposed research aims to study a HO schemes in the WiFi/WhiteFi integration environment. To support mobility between WiFi/WhiteFi, we consider the use of the FMIPv6 protocol and the IEEE 802.21 standard, which provide information about neighboring networks. With MIH help, we propose two scan schemes trying to solve the delay issue of WhiteFi scan process. By reducing scanning time, the performance of the whole HO process will improve. The performance will be analysis based on an analytical model that assesses HO delay.

1.5 Research Methodology

To achieve the desired objectives, this study follows the following steps:

1. Study the structure, properties, and associated procedures of WiFi and WhiteFi technologies and make comparisons.
2. Review issues related to the HO process including issues such as HO definition and types, HO steps, decision algorithms, mobility protocols, MIH standards, and the performance matrix.
3. Consider cross-layer concepts, e.g., using MIH to optimize the mobility protocol, such as FMIPv6.
4. Compare existing literature for seamless HO integrating MIH and FMIPv6.
5. Develop the key signaling mechanisms that are proposed in the context of HO schemes between WiFi and WhiteFi.

6. Evaluate the performance of the abovementioned mechanisms using a detailed analytical model in term of total HO delay.

1.6 Thesis Organization

The thesis is organized into seven chapters. Chapter 2 introduces the background to wireless networks, with emphasis on the IEEE 802.11 standard; discusses mobility and HO issues; reviews mobility management protocols; and explains the MIH protocol. Also, Chapter 2 discusses the TVWS bands used by secondary users (SUs) under regulatory rules provided by the United States (US) Federal Communications Commission (FCC). The new standard IEEE 802.11af, which uses TVWS, is also discussed in Chapter 2. Chapter 3 reviews the work conducted to enhance the HO process using the MIH protocol for different networks and presents improvements to different network layers. Chapter 4 discusses the proposed schemes and the HO scenarios between WiFi and WhiteFi networks. The chapter includes the analytical model and data to be used in the evaluation and analysis. Chapter 5 presents the results of the proposed work, while Chapter 6 analyzes these results. Finally, Chapter 7 presents the conclusions of our proposed work and suggests directions for future work.

Chapter 2

Background

2.1 Introduction

Nowadays, as the number of wireless access technologies is rapidly increasing, the MN can choose to connect to the best available network to achieve the Always Best Connected (ABC) concept. Performing HO to another network is optional if the MN detects a new network while its current serving network connection is good. The decision depends on various criteria related to networks and the MN such as better services, less cost, user preference, and MN battery. HO is mandatory when the MN needs to move across networks to maintain its internet services. HO between the same technologies, e.g., WiFi–WiFi, is called a horizontal HO (HHO), while HO occurring between different technologies, e.g., WiFi–WiMAX, is known as vertical HO (VHO). There are many issues related to the HO process such as scanning delay, IP address changing, packet losses, and choosing the target network to perform HO.

The FCC allows the use of TVWS channels, which includes unused licensed radio channels, by SUs (unlicensed users) with some conditions. Resources of networks operating on TVWS are limited terms of time and availability because PUs (licensed users) have priority. Therefore, the MN may not always be able to connect to a network via a specific TVWS channel in the presence of its PU or it may have to release the TVWS channel if a PU requesting this channel is detected and move to another channel or even handoff to another network in case of no channel available.

WiFi, in its current standardized form, (IEEE 802.11a,b,g,n) cannot operate on the TVWS band due to the lack of various mechanisms related to the TVWS band usage e.g., mechanisms for protecting the PUs. For this reason, the related IEEE 802 standardization groups have made some amendments to the MAC and PHY layers of the IEEE 802.11 standard and named the modified one “IEEE 802.11af,” which is referred to as "WhiteFi". The integration between WhiteFi and WiFi extends the provision of wireless internet services at a low cost. WiFi has the throughput, while WhiteFi has the range. When WhiteFi networks are designed to cover all areas, a MN can use it whenever the WiFi coverage drops.

The next sections discuss the related concepts to our work: wireless communication, TVWS, mobility, and HO issues.

2.2 WLAN Networks [9]

The IEEE is an American Institute that, among other activities, standardizes various wired and wireless network technologies by developing standards such as IEEE 802.11. The low cost and high performance of IEEE 802.11 have made it attractive and enabled its wide market penetration. More details of this standard are provided in the following sections.

2.2.1 WiFi architecture [10]

WiFi, or the IEEE 802.11 standard, assumes a Basic Service Set (BSS) involving a group of devices (STAs) within the coverage area of one access point (AP). The AP, on the other hand, is connected to a wired LAN. When more than one AP are interconnected via a wired LAN with the same "network name", they form an Extended Service Set (ESS) (Figure 2).

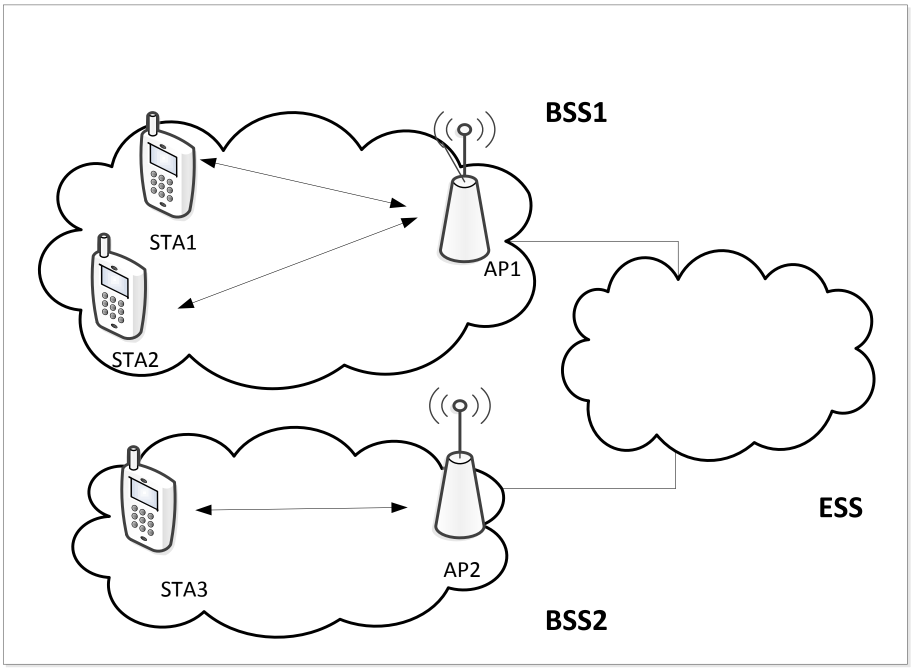

Figure 2. IEEE 802.11 architecture

2.2.2 IEEE 802.11 standards [9, 11]

WiFi includes the following IEEE standards:

- 802.11a: Operating in the 5 GHz ISM band with data rates up to 54 Mbps.
- 802.11b/g: Operating in the 2.4 GHz ISM with data rates up to 11 Mbps for (b) and up to 54 Mbps for (g).
- 802.11n: Operating in the 2.4/5 GHz band with data rates up to 600 Mbps.
- 802.11af: Operating in the 54-698 MHz TVWS band with data rates up to 12 Mbps.

IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n operate in the Industrial, Scientific, and Medical (ISM) band. The 2.4 GHz (2.400 GHz ~ 2.4835 GHz) ISM band provides 83.5 MHz of continuous radio spectrum. The 802.11 standard is divided into 11 channels. To avoid interference, only three of the available channels can be used (1, 6, 11). In Japan, the number of channels is extended to 14 with four non-interfering channels. IEEE 802.11a and IEEE 802.11n operate in the 5 GHz band; the channels are spaced 5 MHz apart.

2.2.3 Association procedure [12]

The IEEE 802.11 standard provides two options for a device to scan neighboring networks and select an AP with which to associate (Figure 3).

- **Passive Scanning (Mandatory)**

  Each AP sends a beacon periodically (10 beacons per second) to introduce itself to others. A device or MN scans all the channels to listen to the beacon messages. None, one, or more than one message may be found. If many APs are found, the MN selects the best one. This is followed by an authentication (if needed) and association request/response messages exchange.

- **Active Scanning (Optional)**

  The MN does not wait for beacons. Instead, it initiates the association process by sending probe frames on each channel and wait. In result, all APs that can serve it will respond to those probe frames with Probe Responses to initiate the process. The MN then selects the best AP from the list. Active scanning creates additional traffic, i.e. meaning more network resources have to be used and more device battery power has to be consumed.

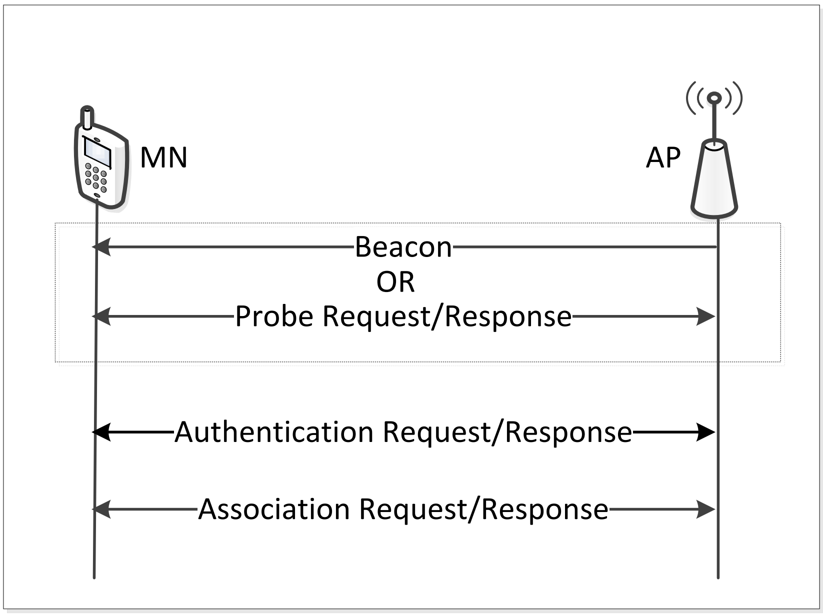

Figure 3. IEEE 802.11 association process

2.2.4 HO procedure

Even when an MN is associated with its AP, it still listens to other AP beacons. When the MN finds an AP with a better signal, it sends a re-associate request message containing information about the MN and its current AP. The current and new APs (NAPs) communicate to attach and complete the HO process with IEEE 802.11f help, the Inter Access Point Protocol (IAPP). To reduce the HO time between two WiFi APs at the same domain while maintaining a secure association, IEEE 802.11r is used. The MIH (IEEE 802.21) standard was developed to help in the HO between IEEE 802 and non-IEEE 802 wireless networks.

2.3 TV White Space [7, 13]

TV broadcasting uses Very High Frequency (VHF) and Ultra High Frequency (UHF) bands (30 MHz to 1000 MHz). In some locations, some of these frequencies are unused at certain times. The US FCC named the unused TV spectrum "White Space". Between January 2004 and August 2005, only 5.2% of the TVWS spectrum was used in the US (on average), meaning that resources were being wasted despite the lack of resources in rural and remote areas [14].

Because some parts of the TVWS spectrum are not constantly used by licensed users (PUs), the FCC allows unlicensed users (SUs) to access the TVWS according to specific rules. Therefore, SUs can take advantage of this band when it is not being used by PUs; however, the availability of TVWS changes over time at any given location. Efficient coexistence of SUs with PUs requires spectrum sensing and spectrum management; thus, the SU MNs must detect when the channel is free to use and be ready to release it when a PU accesses it. A TVWS database plays an important role in this part, as it provides a list of the channels that are not occupied by PUs in specific geographical areas.

The TVWS band is attractive due to its propagation characteristics, coverage, ability to penetrate walls, and large bandwidth. IEEE 802.22 and IEEE 802.11af are examples of standards that use this band. In the future, many wireless networks may use TVWS and, because of its extensive coverage, the networks may interfere with each other, thus affecting the Quality of Service (QoS). For that, coexistence between these heterogeneous systems is required. IEEE 802.19 is a coexistence standard that helps unlicensed heterogeneous systems to discover each other, communicate, and use TVWS effectively.

Systems that use TVWS are referred to as cognitive radio (CR) systems because they use CR techniques for “dynamic spectrum access,” which is a particular area of the CR field, in order to use the unused spectrum (TVWS). These techniques include spectrum sensing and geolocation databases [15, 16].

Two regulators, Office of Communications (Ofcom) in the UK and the US FCC, have set rules regarding how an unlicensed device can use TVWS. Both regulators aim to protect the PUs using databases.

2.3.1 FCC regulation[7]

The FCC defines two types of devices: fixed devices and personal-portable devices. Fixed devices should register their location in the database, while personal-portable devices should only register their devices if they work independently from the control of another device. On the other hand, if a personal-portable device is under the control of a master device, it should not register. "Mode II" device is a master personal-portable device while "Mode I" device is the personal-portable under the control of "Mode II" device. The FCC has divided the band into 51 channels and prevents unlicensed operation on four of the channels. Moreover, it allows only fixed devices to operate on 17 channels; the remaining 30 channels are available for use by all device types including portable ones.

The FCC therefore allows portable devices to operate on 30 channels. According to [17], the average number of channels available for portable devices in rural and urban areas is 18.54 and 9.63, respectively, which represents 61.8% and 32.1% of the available 30 channels.

The FCC has determined the transmitter antenna height and the maximum transmitter power for each type as an extra protection technique for PUs. Furthermore, the FCC has set rules for devices operating adjacent to a channel occupied by a licensed service. All systems that are developed to operate on the TVWS band must follow these regulations.

2.3.2 IEEE 802.22[14, 16]

The first standard using TVWS for wireless regional area networks (WRANs) is IEEE 802.22. The target of this standard is to supply rural areas with lower cost wireless broadband access using the existing technology performance of urban areas. However, this does not mean that systems in urban and suburban environments cannot use it. Small office/home office (SOHO) is an example of target markets addressed by 802.22 systems. IEEE 802.22 is based on CR techniques and its specifications are shown in Table 1.

Table 1. IEEE 802.22 Specifications

IEEE 802.22	
Band	TVWS
Licensed	YES
Type	WRAN
Frequency	54–72, 76–88, 174–216, 470–806 MHz
Bandwidth	6,7, 8 MHz
Max data rate	Max: 22 Mbps

2.3.3 IEEE 802.11af

According to [18], IEEE 802.11af, also referred to as Super WiFi, WiFi 2.0, and WhiteFi, is the first international standard for TVWS WiFi due to its relation with 802.11. The authors of [18] have been heavily involved in Task Group af (TGaf) which formed by 802.11 Working Group (WG) in 2009 to define the changes needed for 802.11 (both PHY and MAC layers) to access TVWS.

As a technology using TVWS, IEEE 802.11af is based on CR techniques that use sensing and databases to make efficient use of the spectrum. Based on the draft of IEEE 802.11af standard, [18] presented the world's first TVWS WiFi prototype.

2.3.3.1 Architecture

The WhiteFi specification is explained in depth in [19]. The main components in IEEE 802.11af, as shown in Figure 4, are a geolocation database (GDB), a registered location secure server (RLSS), and several Geolocation-Database-Dependent Entities (GDD). GDD entities are divided into GDD-Enabling and GDD-Dependent Stations, which are controlled by a GDB and communicate by using the Registered Location Query Protocol (RLQP) to share a White Space Map (WSM) and channel utilization information. The WSM provides the information from the GDB about available channels and corresponding maximum allowed transmission powers for each available channel in a certain area.

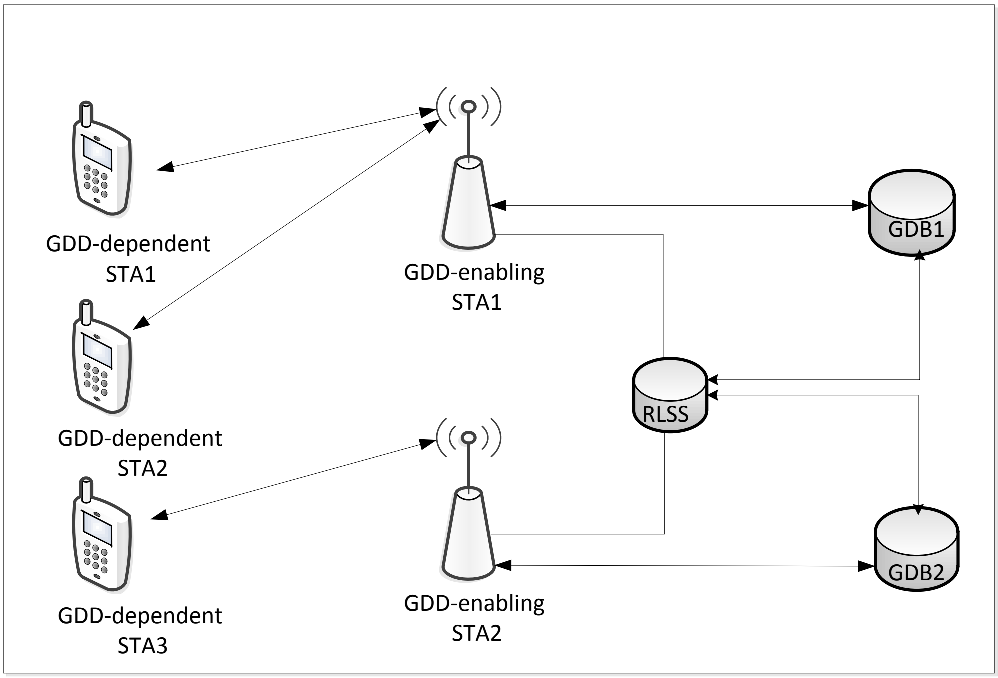

Figure 4. IEEE 802.11af architecture

The **GDB** stores the available frequencies and operating parameters for unlicensed users for each geographic location.

The **RLSS** represents a local database for a small number of BSSs and supplies the GDBs with information on the channels in use by all the BSSs communicating with it. By holding this information, the RLSS plays a significant role as a resource management entity to prevent interference between the APs. APs that connect to the RLSS can make an intelligent decision about which channels to use depending on information provided by the RLSS.

A **GDD-Enabling Station** has the same role as APs but it focuses on which frequencies will be used. For this, it accesses the GDB to obtain the WSM. The enabling station retains an updated map at all times, and it is responsible for validating the WSM at the GDD-Dependent Stations by sending a Connection Verification Signal (CVS). GDD-Dependent Stations send a Channel Availability Query (CAQ) frame to obtain the new channel availability information when it detect a change after comparing CVS information with current WSM.

A **GDD-Dependent Station** is controlled by an enabling station (AP) from which it obtains a WSM and a CVS. The CVS enables the WSM to be verified.

2.3.3.2 Association process

The MN (GDD-dependent STA) cannot perform active scanning by sending a probe request because of the nature of TVWS as a licensed band that protects PUs. An enablement procedure should therefore be performed in accordance with the FCC rules. This procedure is shown in Figure 5. A GDD-enabling STA sends a beacon called “GDD enabling beacon signal” periodically on the available channel containing the WSM. After receiving this beacon on one or more TV channels by passive scanning, the MN can choose one and send a “GDD Enablement Request” frame after association and authentication. The MN waits for a successful GDD Enablement Response to start the connection.

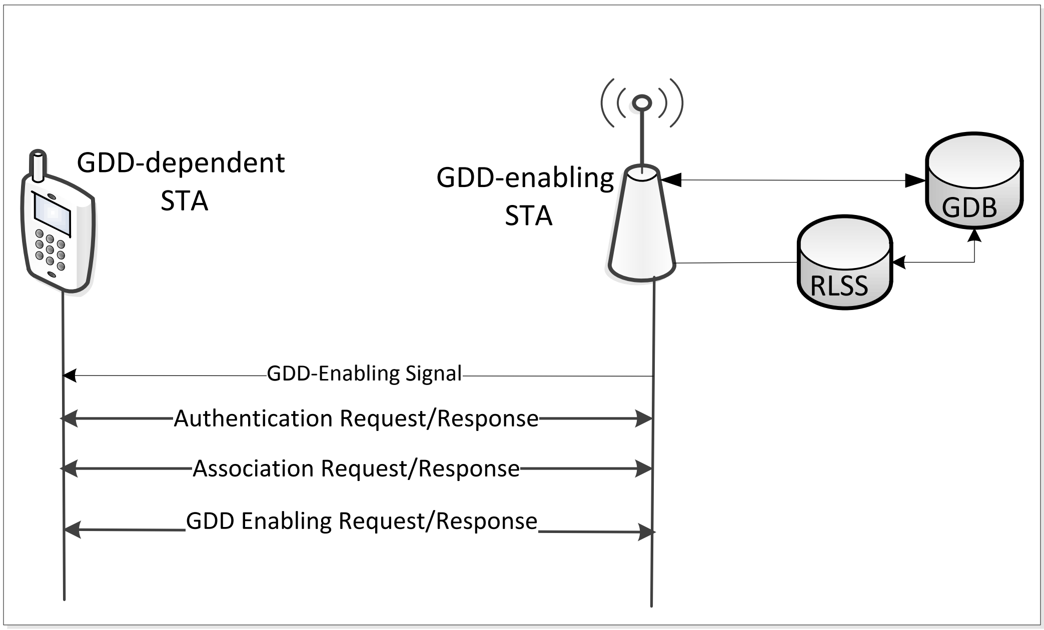

Figure 5. IEEE 802.11af association process

2.3.3.3 Enablement states

Figure 6 summarizes the states of a MN (GDD dependent STA). At the initial state, the MN is in the “GDD Unenabled” state, which means that it is not connected to an AP. It passively scans the channels looking for beacons. The second state is “Attempting GDD Enablement,” which occurs when the MN receives a beacon “enablement signal.” The MN then sends an “enabling request” and waits for a successful response. If no response is received or the MN receives an unsuccessful response, the MN state changes to “GDD Unenabled.” If a successful response is received, the state will be “Enabled” and the connection starts. The MN sets the timer and resets it every time a WSM is received or validate from current AP. When the timer expires, the connection ends (according to the regulations), and the status returns to "Unenabled." The connection also returns to an "Unenabled" state when the AP decides to end the connection.

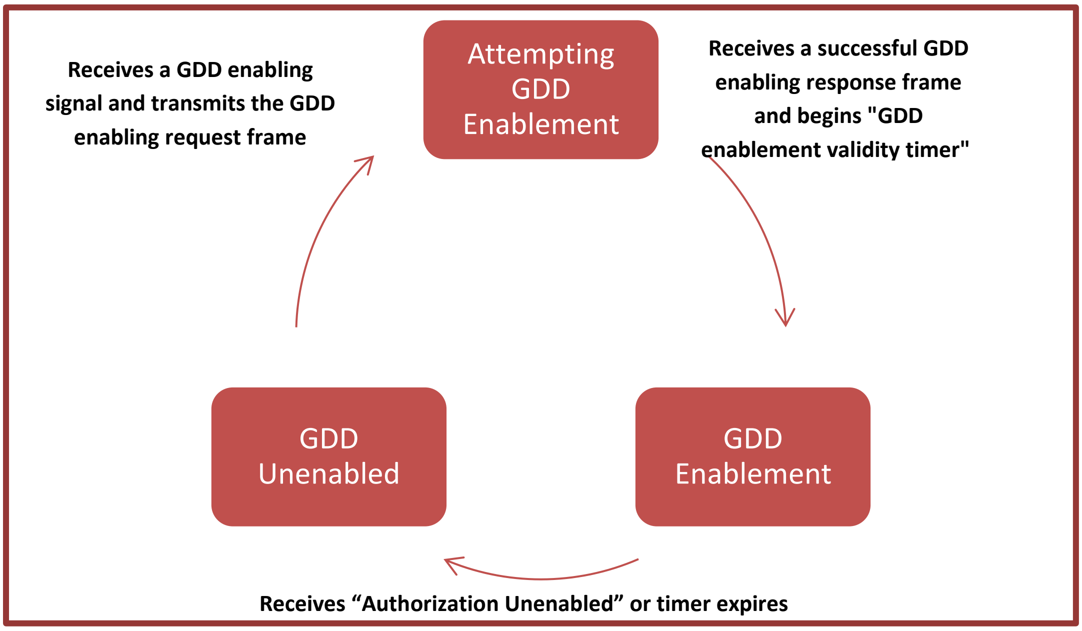

Figure 6. Three enablement states of the GDD-dependent STA

2.3.4 IEEE 802.11af vs. IEEE 802.22

A comparison between IEEE 802.11af and IEEE 802.22 standards can be found in [20], which concludes that IEEE 802.22:

- is the most complete standard, but more costly and complicated
- may serve as a base for "WhiteFi"
- enables high-speed wireless technology in rural areas

Because of early commissioning and the concentration of WhiteFi consumers in cities—where the request for wireless technology is increasing rapidly—IEEE 802.11af is the most promising technology.

Owing to the relationship between WiFi and WhiteFi, the competition between wireless service providers (WSPs) of WhiteFi will increase to offer high-quality services to the customer. Like WiFi, WhiteFi can offer wireless services at popular public sites like coffee shops, stadiums, libraries, and airports. Therefore, WSPs might work together to attract customers to use TVWS networks instead of traditional WiFi hotspots. That may be done by presenting low usage cost opportunities with an acceptable QoS to the customers [21].

2.3.5 IEEE 802.11af vs. IEEE 802.11a/b/g/n

The main specifications differences between WiFi and WhiteFi are presented in Table 2.

Table 2. Comparison of IEEE 802.11 Standards

	WiFi [11]				**WhiteFi[20]**
802.11	b	g	a	n	af
Band	ISM				TVWS
Licensed	NO				YES
Type	WLAN				
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4/5 GHz	54~72,76~88,174~216 470~698 MHz
Bandwidth	22 MHz	20 MHz	20 MHz	20/40 MHz	6 MHz
Max data rate	11 Mbps	54 Mbps	54 Mbps	$\leq$ 289 at 20 $\leq$ 600 at 40	Max: 12 Mbps

The performance of WhiteFi in rural and urban areas is studied in [22]. The study presents a comparison between WiFi and WhiteFi in these environments regarding the following items:

- **Coverage**

  WhiteFi's wide coverage decreases in a high urban environment due to the increased user density. This is because AP should decreased transmitter power to avoid decrease the throughput in result of collision avoidances.

- **TV Channel Availability**

  The larger number of available TVWS channels may lead to higher throughput, compared to the ISM based WiFi. However, with the increasing number of active users, the transmitter power is forced to decrease to avoid interference, thus leading to decreased throughput. In general, ISM band throughput—which is used by traditional WiFi—is higher than the throughput achieved in TVWS; In fact, 16 unoccupied TV channels are needed to achieve a higher throughput in TVWS systems, considering the aggregation of two (8 MHz wide) TVWS channels compared to the ISM band in urban area. A combination of four or more 8 MHz TV channels can outperform WiFi with 20 MHz in the ISM band.

- **TV Signal Strength**

  In rural cases, with a strong signal, the power transmission will reach its maximum value and the average throughput will increase; however, when the signal is weak, both power and throughput decrease. The signal strength does not affect average throughput in urban areas since the transmitter power is always within the same range, regardless of the strength of the signal. That is because even when the signal is good (large coverage), the probability of collisions is high; therefor to avoid collision the coverage should decrease, resulting in a reduced transmitter power requirement.

2.4 Network Integration Challenges

The HO is the most challenging process related to network integration. Issues related to the time when the MN decide it needs to HO, time to actually execute the HO, and the criteria by which MN chooses the target network need to be considered for the MN to move between these integrated networks while maintaining the same quality of connection. Also, the HO should be executed with minimum packet loss and delay. The next section discusses HO-related topics in more detail.

2.4.1 Handover [23]

HO and roaming are terms that describe the procedure of changing the connection of an MN from one cell to another. This change occurs due to the movement of the MN among different networks, because either a current network link is going down or a new network link is detected with a better signal strength.

2.4.1.1 HO types

As mentioned previously, if the MN moves between the same technologies (e.g., WiFi–WiFi), the HO is called Horizontal HO (HHO), while the Vertical HO (VHO) occurs between different technologies (e.g., WiFi–WiMAX). Many layers such as L2 (link layer), L3 (network layer), L4 (transport layer), L5 (session layer) and L6 (application layer) may be involved in the HO process. HO is divided into soft and hard HO. Soft HO (make-before-break) maintains the existing L2 connection that is still valid until the new one is established, while a hard HO (break-before-make) breaks the existing connection prior to establishing a new one. The most important advantage of a soft HO is that no packet loss occurs during the HO, but it requires increased resources in both MN and the APs.

2.4.1.2 HO process

1. HO information gathering

The HO information gathering phase is the first and very important phase since the data collected during that phase will be used in the second phase, the decision phase. The information gathered in this phase is as follows:

- Available networks link information: throughput, cost, packet loss ratio, received signal strength, noise signal ratio, signal to interference ratio, bit error ratio, distance, QoS parameters, and HO rate.
- Mobile device (MN)information: battery, speed, service class, and resources.
- User preferences: budget and services required.

This step is critical to the HO procedure. The decision taken about the need to HO, when to HO, and the target network will depend on these data.

2. HO decision

Having the best possible connection in an environment of multiple access technologies is related to the "ABC" concept. For that, a HO management technique must choose the most suitable time to initiate the HO and the most suitable access network for a specific service among those available. Service continuity must be maintained. In this phase, the gathered data is processed and evaluated, and the decision is made about when the HO will be triggered and to which network the MN will be switched. To achieve the correct decision, some criteria can be used to help determine which access network to select. For example, received signal strength, bandwidth, latency, monetary cost, security level, battery power, user profile and preferences, and QoS. The HO decision depends on the received signal strength

(RSS) in HHO. A VHO is more complex because more parameters need to be assessed to make the right decision; thus, algorithms with certain criteria are used to choose the best network.

A recent review of existing algorithms, which were proposed in [24], found that simple algorithms that depend on signal strength will perform seamless VHO with small delays but with lower throughput. On the other hand, complex schemes, which use an artificial intelligent (AI) approach, and schemes using multiple parameters, such as cost and QoS, improve the throughput but with increased HO delays.

Based on the HO decision criteria assumed and the methods used, [25] classifies decision algorithms into four groups: RSS-based algorithms, bandwidth-based algorithms, cost function-based algorithms, and combination algorithms. Some of these algorithms are general and can be applied to any two heterogeneous wireless networks; whereas, others apply to only two specific networks. The [25] presented a comprehensive survey of these algorithms and found that the currently proposed VHO decision algorithms either lack a comprehensive consideration of various network parameters or the studies reporting these algorithms lack enough detail for implementation.

3. HO execution

After selecting the target network, the HO is initiated. Execution of the HO includes controlling the signaling changing (L2), and may include higher layers if necessary such as the IP address and/or session changes,.

2.4.1.3 HO performance

The performance of the HO process is assessed by metrics such as the number of successful HOs, HO delay, end-to-end latency, packet loss, and signaling (messages exchanged to perform the HO) overhead.

2.4.2 Mobility protocols

As previously mentioned, HO is required when the MN moves among networks. When both the old and new networks are in the same domain, it is considered micro-mobility. Macro-mobility is the movement of the MN between different domains or between different technologies. While the MN can change its physical link from one access network to another, its IP address should change due to the change in the point of attachment. It is important to manage this change dynamically, with uninterrupted communication. Solutions to support mobility at the network layer have been proposed to overcome this limitation. The main idea in the most of the proposals is to create a new IP address for the MN. The IP address is used for routing to the current access network; however, the original address is still used as an identifier for management. The traffic sent to the original address will not be lost; it is just delivered via the new address to the MN [26, 27].

The Internet Engineering Task Force (IETF) proposed the Mobile IP (MIP) standard, which is the most frequent solution for supporting mobility at L3. MIPv6 and MIPv4 are versions of MIP.

2.4.2.1 MIPv4 and extensions

In MIPv4, a foreign agent (FA) is located in every visited network, which is responsible for generating a new IP address, referred to as Care-of-Address (CoA), which changes with every new subnet visited. A Home Agent (HA) is the entity located in the home network, which is responsible for keeping information about the CoA of the MN. In MIPv4, MN informs the HA about its new CoA with the FA's help. MIPv4's latency is unsuitable for real-time applications and multimedia. The delay is caused by the separation of L2 and L3 since the MN cannot communicate with FA until L2 HO finishes. Therefore, the following extensions have been developed.

- **Low Latency Handover (LLH)**

  LLH can solve the delay problem by applying cross-layer techniques between L2 and L3. The most advanced method used in LLH is Pre-Registration. In this process, FA keeps a mapping table of other FA’s IP addresses with L2 identifications.

- **Mobile IPv4 Fast Handovers (FMIPv4)**

  While the HO is performed, the MN sends and receives data via a connection between the previous (PARs) and the new access routers (NARs). The old access router should use the L2 address of the new AP to extract the IPv4 address of the new access router.

2.4.2.2 MIPv6 and extensions

Some differences exists between MIPv6 and MIPv4. MIPv6 allows the MN to generate its own CoA and directly informs the HA about the new CoA, meaning that the FA is no longer required. The MN knows about the change of its location by router solicitation/advertisement messages with the NAR. The new CoA should be tested for duplicates following the Duplicate Address Detection (DAD) procedure. DAD is conducted by exchanging neighbor solicitation/advertisement messages. After that, the MN exchanges binding update/acknowledgment (BU/BAck) messages with the HA, and the Return Routability (RR) procedure is executed based on testing the home address and the CoA. The last step involves exchanging BU/Back with all active corresponding networks.

- **Fast HOs for MIPv6 (FMIPv6)**

  The main goal of FMIPv6 is to reduce the HO latency of MIPv6. It operates in Predictive and Reactive modes. An L2 trigger is used to detect the HO. To generate a CoA, the MN exchanges router solicitation/advertisement messages with the PAR, called RtSolPr/PrRtAdv, which brings information about the NAR to help with CoA generation. The MN now sends a fast binding update (FBU) to the PAR to associate the CoA with the home address. HI/HAck messages are exchanged between the NAR and PAR. An FBU acknowledgment (FBAck) is sent to show the validity of the CoA from the PAR to the NAR and the MN. After exchanging the HI/HAck between the NAR and PAR, a tunnel is created between them. The PAR forwards any packet destined for the MN to the new CoA via the NAR, which in turn forwards the packets to the MN when the MN attaches to it, after the MN has sent a Fast Neighbor Advertisement (FNA). These steps describe the procedure of the predicted mode of FMIPv6.

  The reactive mode happens when the MN does not receive an FBAck message on the link with the PAR, which occurs when the MN does not send an FBU or because it dropped the link after sending an FBU. The MN sends an FBU with a FNA to attach to the NAR. After checking the CoA, the NAR forwards the FBU to the PAR. The PAR will respond with an FBAck. In that way, the packets are forwarded to the NAR, which the NAR forwards to the MN.

- **Hierarchical Mobile IPv6 (HMIPv6)**

  The target of HMIPv6 is to enhance micro-mobility efficiency. This is done by reducing signaling, limiting the delay, optimizing routing, and improving scalability. The standard adds entities that serve local HOs (micro-mobility) called Mobility Anchor Points (MAPs). MAPs is similar to the HA in MIPv4 but it can be located anywhere in the router's hierarchy. A MAP uses three addresses: home address, on-link CoA (LCoA), and Regional CoA (RCoA).

If the MN moves between networks belonging to the same MAP or access network, a BU is does not need to be sent to the HA. A BU is sent to the MAP only if the LCoA changes. When the MN moves between two MAPs, the HA should know about this movement and a BU should be sent.

- **Proxy Mobile IP(PMIPv6)**

Network-based IP mobility management is provided by PMIPv6, where the MN is not involved in IP-related signaling. Three entities includes in this protocol:

- Authentication Authorization and Accounting (AAA) Server manages the authentication and maintains the profile of the MN.
- Local Mobility Anchor (LMA) is the HA for the MN that forwards traffic to and from MNs.
- Mobile Access Gateway (MAG) follows the MN's movements and signaling of the MN's LMA.

The MAG detects the MN's movement and obtains a profile from the AAA server. The MAG sends a Proxy BU (PBU) to the MN's LMA, which queries the AAA server. Once a reply is received from the AAA server, the LMA updates the binding cache entry with the new MAG address. The LMA sends a PBU acknowledgment to MAG, which sends a router advertisement to the MN.

Finally, Fast PMIPv6 (FPMIPv6) is develop to optimize PMIPv6. During the HO, a direct tunnel between Previous MAG (PMAG) and Next MAG (NMAG) is used to forward traffic. When the MN is disconnected during the HO, its downlink data may be buffered in the NMAG.

2.4.2.3 MIPv6 protocols comparison

[27, 28] present an evaluation of the different MIPv6 extensions protocols. They show that some protocols are superior to others, according to the following specific performance parameters:

- Reduction of HO latency: FMIPv6 and FPMIPv6 have less latency because they use L2 triggers to begun execute before actually L2 HO execute. The latency reduction results in reduced HO blocking probability. MIPv6 and HMIPv6 have more latency because of the DAD process.
- Packet loss: FMIPv6 and FPMIPv6 have less packet loss because buffering during L2 HO at NAR/NMAG results in a reduction of lost packets.
- Signaling cost: PMIPv6 and FPMIPv6 are better because their nature as network-based protocols reduces signaling; thus, the MN is not involved in the signaling procedure.

Table 3 shows the comparison of mobility protocols in terms of HO latency, packet loss, signaling cost, and blocking probability:

Table 3. Comparison of the Performance of MIPv6 Extensions

	FMIPv6 predictive	FMIPv6 reactive	HMIPv6	PMIPv6	FPMIPv6 predictive	FPMIPv6 reactive
HO latency	*				*	
Packet loss	*	*			*	*
Signaling cost				*	*	*
Blocking probability	*				*	

2.4.3 IEEE 802.21: MIH [8]

To make a generic interface for HO, IEEE 802.21 was developed. IEEE 802.21 provides an MIH protocol to enable seamless HO between different technologies. It provides information like L2 (data link layer) triggers, current link status, and new link detected to L3 (network layer) and above to help in the HO decision phase. IEEE 802.21 does not dictate rules or algorithms for selecting a target network. It merely helps to discover networks, prepare target networks, and initiate an L2 HO. It does not perform the HO itself.

To get the advantages of MIH, the MN and involved networks should have MIH capabilities. An "MIH Capability Discovery" primitive is used to discover whether the entity supports MIH and determine the supported services.

2.4.3.1 MIH reference model

As Figure 7 shows, the IEEE 802.21 standard defined a functional entity called a Media Independent HO Function (MIHF), which is an abstraction layer, called L2.5, because it exists between the upper layers (L3, L4, etc.) and the link layer (L2) of the different wireless technologies. To communicate with the MIH users (mobility management protocols) and L2 interfaces, MIH defines three service APs (SAPs):

- MIH _SAP: MIH users with MIHF
- MIH_LINK_SAP: data link of different technologies with MIHF
- MIH_NET_SAP: local MIHF with remote MIHF

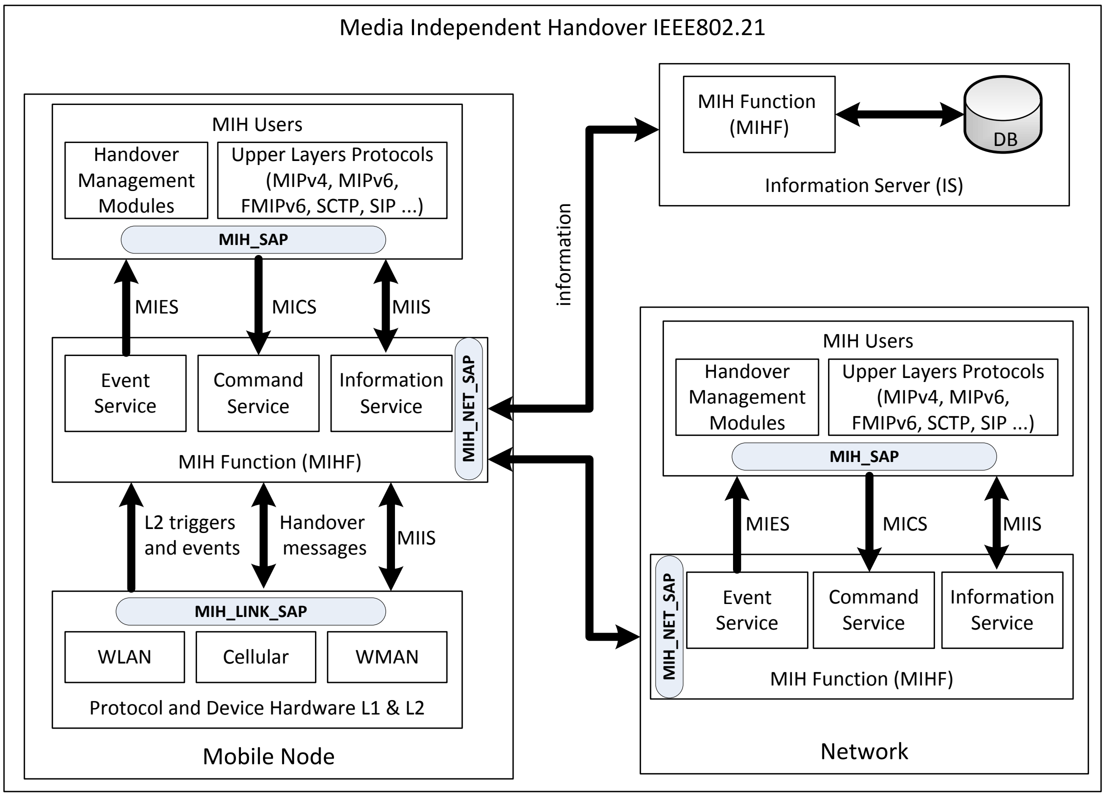

Figure 7. IEEE 802.21 reference model

2.4.3.2 MIH services

- **Media Independent Information Service** (MIIS)

  MIH assists in the HO decision via MIIS, which provides information about available networks within the area to the upper layer using an Information Server (IS) containing all data about local networks. These information elements (IEs) are divided into three main groups: (1) access network information, such as types and cost; (2) PoA information for each AP in each access network, such as address, data rate, and location; and (3) specific information, such as vendor specific data. MIIS communicates with the IS using the MIH_Get_Information primitive to obtain these data in the form of an IE structure.

- **Media Independent Command Service** (MICS)

  The commands can be local, from the upper layer to the lower layer, or remote, between the MN and the access network. An MIH user can control the link behavior related to HO requirements by these commands: MIH Scan, MIH Handover Initiate, and MIH Get Status.

- **Media Independent Event Service** (MIES)

  This service notifies the changes in state and quality of the transmission of physical or link layers, referred to as “Link” events and “MIH” events. The difference between these events is that Link events are exchanged between MIHF and interfaces, while MIH events are exchanged between MIHF and upper layers or remote entities. Link_Detected, Link_Handover_Complete, and Link Parameters Change are some examples. A Link_Going_Down event is an example of predictive mode, while Link_Up and Link_Down events are related to the reactive mode that inform the MIHF when a link is up or down.

2.5 Conclusion

We have presented the WiFi and WhiteFi architectures in this chapter and introduced the HO issues, mobility management protocols, and MIH protocol. In the next chapter, we will explain some of the existing solutions that used MIH protocol to improve the HO performance focusing on works done with WiFi to adapt them for WhiteFi /WiFi integration.

Chapter 3

Literature Review

3.1. Introduction

Many proposed enhancements of HOs among WiFis, or among WiFi and different standards, use the IEEE 802.21 protocol. MIH is the HO protocol that provides the enablers for performing a HO between IEEE 802 and non IEEE 802 networks. IEEE 802.21 assists in searching for new links and setting them up. The standard does not specify when or how the HO decisions are made and it does not include the HO execution mechanisms. Many papers presented in this chapter used MIH in their proposed models and observed the performance enhancements of different layers.

The MIH primitive (MIH_Link_Going_Down) is used as an HO trigger. The link status and MIIS information help to improve decision algorithms in order to make the right decision about the target network and the right time to initiate HO. The MIIS plays a big role in decreasing the network scanning time and, thus, the total HO delay.

The performance of mobility protocols, including FMIPv6 which is explained in section 2.4.2.2, can be enhanced by using MIH. For example, [8] shows that MIH can help to solve the ping-pong effect , where the MN performs many handovers between the same cells back and forth, in a short time period, in MIPv4 by starting the execution only when MIH_Link_Going_Down events occur. In addition, with the information obtained from the MIIS server, the solicitation/advertisement messages are eliminated, thus reducing the HO delay. Enhancements in the HO performance using the services provided by MIH are presented in the literature works discussed in this chapter.

3.2. MIH Based HO

The MIH protocol has been developed to help VHO between 802 and non-802 networks, but HHO is also supported. For example, MIH can help in the scanning phase, which causes much of the HO delay time among WiFi networks. MIH was used in HHO between WLANs to improve this phase. The works explored in Section 3.3.1 show how the MIIS can reduce this delay**.**

A VHO between WiFi and Universal Mobile Telecommunications System (UMTS) is performed with and without MIH in [5]. The paper showed that the HO delay in the soft model (using MIH) is reduced compared to the HO delay in the hard model (without MIH) by 8%. By contrast, this delay increased when the number of MNs increased. With MIH services, the packet loss is avoided if the network load was below 384 kbps (saturation point of UMTS).

In [4], the authors studied the performance of WiFi/WiMAX HO using MIH. They showed that MIH was not suitable for real-time applications because the throughput, packet loss, and HO latency decreased when the MN speed increased. The authors in

[4] justified these results using the criteria of the decision algorithm in their simulation. The decision algorithm depended only on RSS; thus, they suggested focusing on the decision phase to enhance the QoS. [29] presented an MIH based HO between WiFi and WiMAX, which used SINR instead of RSS in the decision algorithm. The simulation results showed that SINR-based HO provided a higher system throughput compared to RSS-based HO, especially with high data rates.

3.3. HO Enhancement

MIH services can be used to enhance the overall performance of the HO process in different stages. According to [8], enhancement was achieved in the scanning phase by reducing its latency using MIIS to obtain information about a new access network.

3.3.1. MIH utilization in the scanning phase

In [30] and [31], the authors examined the use of MIH services to enhance the HHO process between WiFi APs. The study focused on using MIIS to decrease the scanning phase delay by reducing the number of channels to scan; only the active channels listed on the MIIS server (or subset of them) were scanned. According to the Intelligent-ScanAll technique, all the received channels were scanned. In the Intelligent-StopFirst technique, the active channels (in the provided list) were scanned one by one, and the procedure stopped at the first successful channel. Intelligent-ScanAll and Intelligent-StopFirst techniques reduced the delay by 53% and 65%, respectively, compared to the standard technique of “scan all channels”. Other techniques called “Intelligent-ScanOne” and “Intelligent-ScanNone” are presented in [31]. They are extensions of the previously mentioned techniques [30]. The number of channels to be scanned was reduced to one or zero. Using the GPS coordinates of an MN, the MIIS server would return only one channel. The MN could scan this channel "Intelligent-ScanOne" or attempt to execute HO without scanning "Intelligent-ScanNone". Intelligent-ScanOne and Intelligent-ScanNone reduced the delay by 93% and 99%, respectively.

In [32], the authors studied the effect of intelligent scan (Intelligent-ScanOne and Intelligent-ScanNone) on the HO delay of MIPv6. The result showed delay reductions of 82% and 89%, respectively.

The authors in [33] proposed a scheme in which the MN would choose the nearest AP from the list obtained from the MIIS server. Then, the MN would check the RSS of the target AP. If the RSS was above a certain threshold, the MN would actively scan the channel. If the AP responded, the MN would connect to it; otherwise, it would repeat the procedure with the next nearest AP from the same list. The procedure is like the StopFirst scheme.

3.3.2. MIH utilization in the execution phase

For both MIPv4 extensions—LLH and FMIPv4 [26]—the dependence on L2 triggers to initiate a HO cannot rely on IEEE 802.11 messages, because the detection phase takes more than one second. Therefore, pre-registration may not be completed due to the loss of the MN connection with the AP. For MIPv6 extensions, FMIPv6 is more suitable [34] than PMIPv6.

The work in [35] presented experiments with real implementations of MIPv6 and FMIPv6 and evaluated their performance with real applications in an IEEE 802.11g network environment. It showed that the HO latency of the predictive mode of FMIPv6 is the best compared to MIPv6 and the reactive mode of FMIPv6. Due to the short HO time, the packet loss was less in both modes. Concerning jitter (the variation in latency), all protocols have similar jitter, but FMIPv6 in the predictive mode has a (slightly) higher jitter than the other protocols. In terms of video quality, the study measured the quality of the streaming video before and during the HO, using "Mean Opinion Scores" with ten users. Even with jitter, users preferred FMIPv6 because MIPv6 causes the highest delay. Thus, FMIPv6 performed well with real-time or streaming applications. The MIH could interact with the mobility protocol to improve HO performance, as described in the following paragraphs.

The work in [3] proposed an architecture that used the MIH protocol to perform a seamless HO. HO performance was evaluated assuming the use of MIH in the initiation and execution phases. It showed that HO execution delay as well as the total HO delay was reduced by using MIH services. In this work, HO delay is consider as the time between the last packet received on the old interface and the first packet received on the new interface, while HO execution is the time starting from when the BU message is sent from MN to HA until the first packet is received on the new interface. Packet loss was zero, since both connections were available during HO. When MIH was not supported, the old connection ended before the new one commenced.

Considerable research work optimized the legacy FMIPv6 using MIH services. Figure 8 shows the original message flows of the FMIPv6 for both predictive and reactive modes (RFC 5568) :

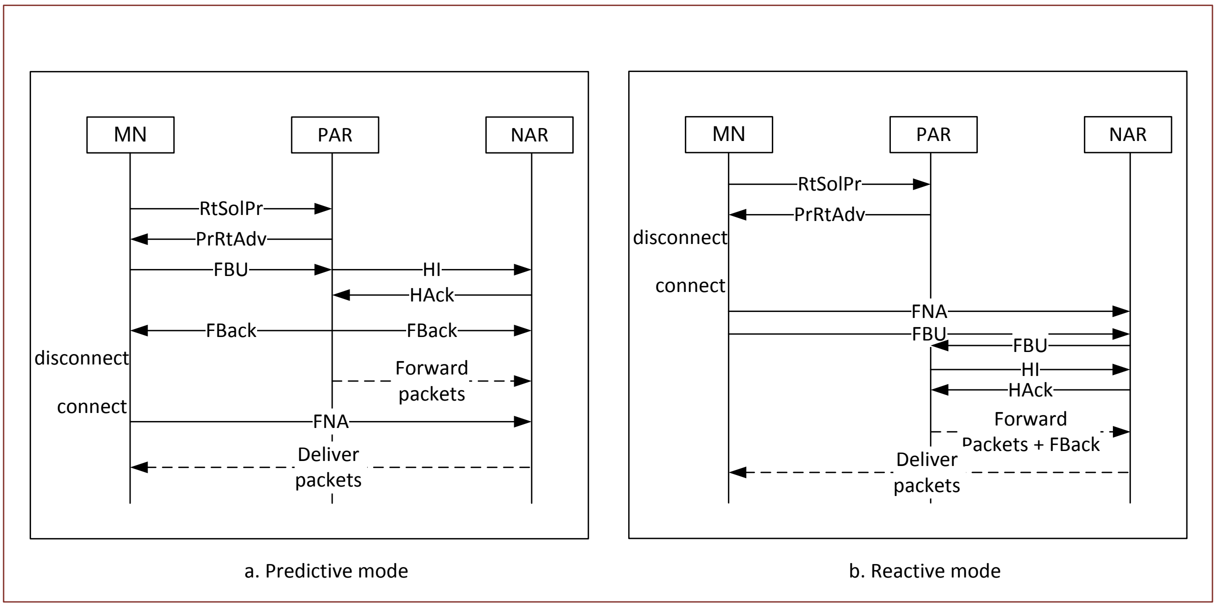

Figure 8. FMIPv6 modes signaling

In [36], PAR redirected packets only when the Link_Down event was received. This allowed the PAR to serve the MN for longer time, thus reducing HO latency. The NAR also used Link_Up event to start forwarding packets to the MN. With the help of MIH, the HO initiation delay was reduced, this was achieved by collecting information about neighboring networks before the need for the HO. Reducing the HO latency in [37] was accomplished by removing (RtSolPr/PrRtAdv) router discovery messages. The information obtained by the IS was used to extract the NAR information. The simulation of HO between WLAN/UMTS using NS2 showed a reduction in the HO latency and the packet loss. Packet loss was zero when the MN moved from UMTS to WLAN.

In [38], the authors proposed a network-based seamless HO using MIH, which reduced the overall number of messages by using new and modified MIH messages. MIH_MN_HO_Profile message was sent to the serving network by the MN to allowing the serving network to obtain information about neighbor APs from IS instead of it. The MN let the serving network choose the target network by sending MIH_MN_HO_Grant. This message replaced MIH_MN_HO_Candidate_Query Request/Response messages. The last change proposed in this paper was to use a local primitive MIH_BindingUpdate, thus negating the need for FBU. The signaling overhead and HO latency were reduced.

Because of the advantages of predictive mode over reactive mode in FMIPv6, in [39], the authors increased the performance of the predictive mode by using MIH to localize the MN for forwarding FBack messages to its new location.

3.4. Summary

Table 4 contains a summary of the related works using MIH to enhance MIP protocols.

3.5. Conclusion

Much of the work presented in literature has aimed to optimize the HO process by maximizing HO performance using MIH. As the scanning phase causes much of the HO delay, especially in HHO, most research has focused on reducing the scanning time by reducing the list of channels to be scanned or even omitting this phase completely. For WhiteFi, this will be more challenging because of the regulations set by the FCC. In L3 HO, mobility protocol, FMIPv6, was enhanced by removing its initial two messages (RtSolPr/PrRtAdv) using MIIS.

According to our research, HO from/to WhiteFi has not yet been adequately studied because it is a new standard. The first objective in this thesis is to develop a mechanism help to reduce the HO delay between 802.11 networks (WiFi–WhiteFi) and study its performance considering the aforementioned works.

Table 4. Summary of Enhancement of Presented Work Using MIH

Paper	Networks	Mobility protocol	MIH service involve in the study	HO phase involve	Evaluation method	Enhanced parameters
[30] [31]	WiFis	---	(MIIS)	Discovery	Simulation NS2	Delay
[33]	WiFis	---	(MIIS)	Discovery	---	Delay
[32]	WiFis	MIPv6	(MIIS)	Discovery using [31]	Simulation NS2	Delay, Packet loss
[3]	WiFi,/ WiMAX/3G	MIPv6	All	Initiation Execution	Simulation	Packet Loss HO delay HO execution delay
[36]	General	FMIPv6	MIIS Link_Up Link_Down	Discovery Execution	Analytical	HO Latency, Buffer Size
[37]	WLAN/ UMTS	FMIPv6	MIIS	Discovery Execution	Simulation NS2	HO Latency Packet Loss
[38]	General	FMIPv6	MIH_MN_HO_Profile MIH_MN_HO_Grant MIH_BindingUpdate	Discovery Execution	Analytical	Signal Overhead

Chapter 4

Proposed Model

4.1 Introduction

This chapter describes the proposed signaling that aims to increase HO performance when the MN is moving between WiFi and WhiteFi networks by reducing the delay of the HO process. We introduce communication between RLSS and IS entities to reduce the delay during the scanning phase, using the MIH protocol. FMIPv6 is used to execute L3 HO because it has less latency compared to MIPv6. FMIPv6 will also benefit from MIH information, which is retrieved from the IS, to reduce the number of exchanged messages by eliminating movement detection (MD) (solicitation/advertisement) messages. The proposed work focuses on enhancing the HO process from WiFi to WhiteFi to fill the gap of previous research.

This chapter includes an analytical model that has been developed to evaluate the performance of the proposed communication between the RLSS and IS when the MN is handed over from WiFi to WhiteFi networks. Finally, model assumptions and corresponding parameters are presented.

4.2 Proposed Network Architecture Topology

WhiteFi has an assumed range of 1 km. Such large coverage can fill the gaps between WiFi networks. The topology of WhiteFi is shown in Figure 9.

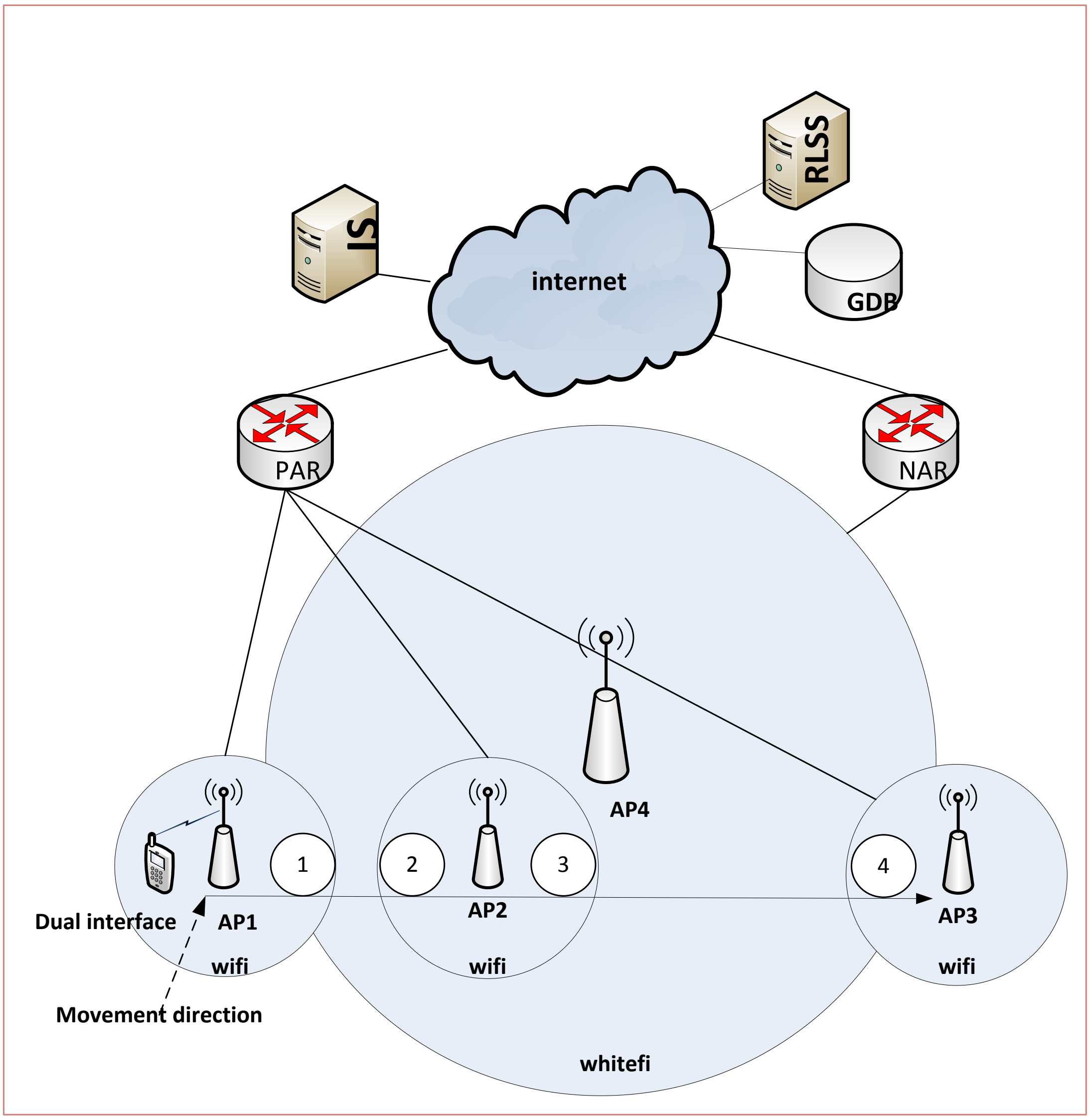

Figure 9 Proposed architecture topology

Abbreviations: AP1, 2, 3: WiFi Access points; AP4: WhiteFi Access point; GDB: Geolocation database; RLSS: registered location secure server; IS: information server (MIIS); NAR: new Access Router; PAR: previous Access Router.

Our topology has three WiFi networks and one WhiteFi network. Two WiFi networks are located on the edge of the WhiteFi network and one WiFi network is situated inside the coverage area of the WhiteFi. The MN has two interfaces to both networks and it is moving in a straight line across all four networks. The IS is an MIIS capable server for using the MIH protocol. The RLSS is a part of WhiteFi architecture. RLSS connects with GDB—another entity of WhiteFi—to retrieve the available TVWS channels.

4.3 HO Scenarios

- **Scenario 1 (mandatory):** From WiFi to WhiteFi: MN enters the AP4 (WhiteFi) area, while AP1's (WiFi) signal is weak; thus, HO from AP1 to AP4 is mandatory.
- **Scenario 2 (optional):** From WhiteFi to WiFi: MN enters the AP2 (WiFi) area, this network detected while the AP4 (WhiteFi) signal is still good. If WiFi can serve MN with same level of WhiteFi or better, HO will be performed from AP4 to AP2 in the case of a low MN speed. If the MN's speed is high, HO will not be performed because of WiFi's small coverage.
- **Scenario 3 (mandatory):** From WiFi to WhiteFi: AP2's (WiFi) signal is weak because the MN is moving away from it and AP4's (WhiteFi) signal is excellent; therefore, a HO from A2 to AP4 will be performed.
- **Scenario 4 (mandatory):** From WhiteFi to WiFi: The MN enters the AP3 (WiFi) area while moving away from AP4 (WhiteFi); AP4's signal is becoming weak. Therefore, a HO from AP4 to AP3 should be performed.

4.4 HO Algorithm

Here, we explain in more depth the algorithms of the above HO scenarios from WiFi to WhiteFi and vice versa. The decision depends on the assumption that WiFi always the prefer network with take into account the speed of MN if there is another choice (scenario 2).

4.4.1 From WiFi (scenarios 1, 3)

When the link of the WiFi goes down, the MN tries to find another WiFi AP to which it can connect. If there is no WiFi available (the case study by this thesis), the MN passively scans for WhiteFi enablement signals (beacon). It should scan all TV channels (30 channels, according to the FCC) to find beacons and then choose the best one (Figure 10-a).

4.4.2 From WhiteFi (scenarios 2, 4)

WhiteFi is not the preferred network for an MN because of the instability caused by the varying levels availability, which are dependent on PU usage. Therefore, as another network (WiFi in our case) is detected, the MN will try to connect with it if the QoS will be retained or improved. Because WiFi performance decreases with increased speed, the HO will not be initiated in the case of high speed mobility. Otherwise, the HO will be executed when possible. The HO to WiFi will be mandatory if the WhiteFi link is going down (scenario 2) and optional, depending on the MN speed, if the WhiteFi link is good (scenario 4) (Figure 10-b).

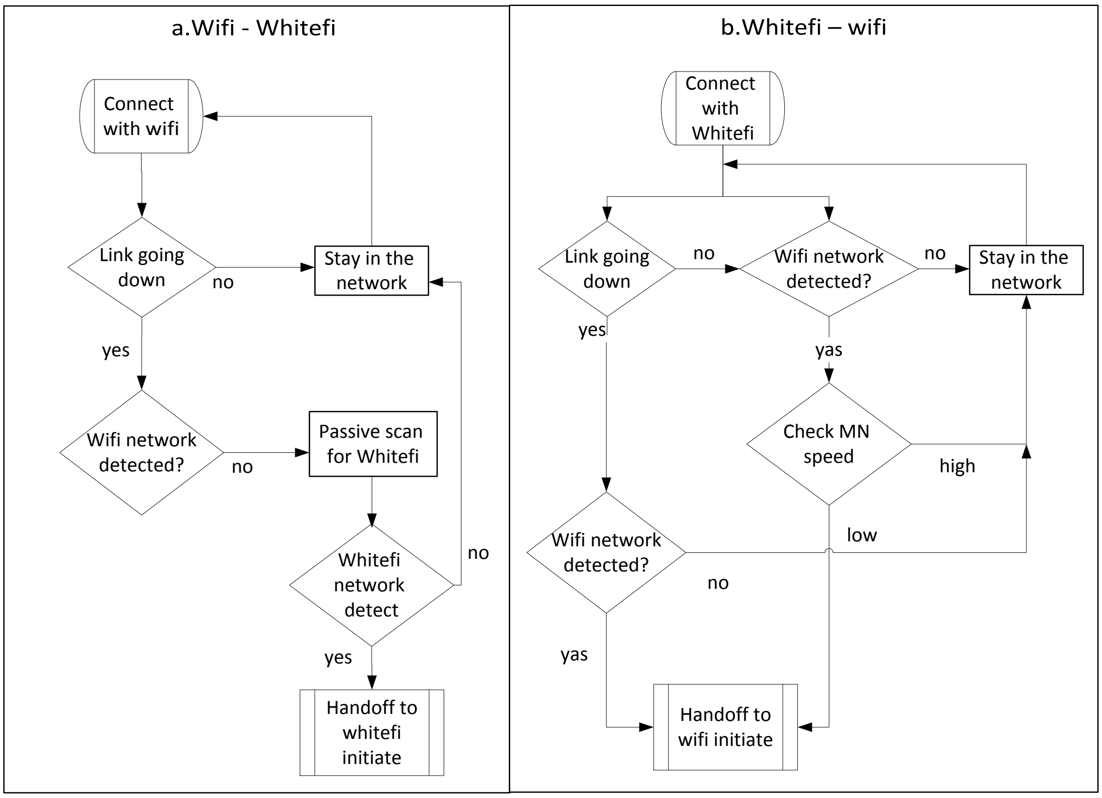

Figure 10. Proposed algorithm of WiFi/WhiteFi HO

4.5 Proposed Model

To improve HO performance, we use the MIH protocol and FMIPv6 protocol as a mobility protocol. MIH is expected to enhance both the scanning and L3 execution phases, as presented in Chapter 3.

4.5.1 IS approach

In MIH, the IS can supply the MN with active channels in its area with related information, which will reduce the scanning time because MN can choose some candidate networks from the receiving list and directly query them to choose one of them. In active scanning, as proposed in [31], the time can be reduced to one or even zero by giving IS the authority to decide on behalf of the MN. IS will receive the exact location and requirements of the MN and choose one target AP to send to the MN. The MN, in turn, will either actively scan the AP channel or start the association procedure directly. Unfortunately, active scan not allow with TV channels. In WhiteFi, the delay cannot be reduced to the level reached by other networks mentioned in the literature. Even if the MN can get a list of active channels in the TVWS band, which are used by APs at this moment, it cannot send a probe request until it receives a beacon. MN only has permission to passively scan them as standard.

4.5.2 IS approach for WhiteFi information

By using the MIH protocol, the existing approach is that IS , as done with other networks , should including WhiteFi information. Even MN cannot actively scan the retrieved channels list, it can get benefit by scanning only those channels being used by WhiteFi APs in the area instead of scanning all 30 channels.

The drawbacks of this approach include the following:

- Increased overhead on the IS server, since the number of incoming messages from APs will increase and the load will be high.
- Unexpected changes in the channels used by WhiteFi APs, due to the appearance of PUs, require more frequent updating of the information of WhiteFi APs in the high rate than other networks types.
- Overload on WhiteFi APs because the AP will double its function; it has to share its information with two servers instead of one server.

4.5.3 RLSS–IS communication

To recover the previous drawbacks , we propose using the RLSS because it already does the job with WhiteFi APs that IS does with all other types of networks. RLSS works as a resource management tool and has access to all information about the WhiteFi APs and the channels used by them in a certain area as well as the TV channels schedule by contacting GDB . Cooperation between IS and RLSS is expected to help reduce scanning delay in WhiteFi networks.

4.5.4 Assumptions

1. The 30 channels that are allowed to be shared with SUs by the FCC can be classified into channels that are occupied by PUs, channels that are occupied with SUs, and empty channels. Depending on this classification we can create these three categories:
   - All: Contains all 30 channels, includes channels that are occupied by PUs, channels that are occupied by SUs (APs and other devices), and empty channels.
   - Free: A subset of all channels, it contains channels that are not occupied by PUs. It includes channels either occupied by SUs (APs or other devices) or empty channels.
   - Active: A subset of free channels, it contains only channels that are occupied by WhiteFi APs.
2. IS always has a copy of Free list (TV schedule) by contacting RLSS and MN can get this list any time contacting IS.
3. IS updates its Free and Active lists by contacting RLSS in two ways:
   - Every 48 h: the Free list is updated at least every 48 h, so at any given time, IS has an updated Free list. MN can get this list whenever it contact IS for periodic query.
   - On request by the MN: In case of HO to WhiteFi, when MN want to reduce number of channels, it ask the IS for Active list. If IS dose not has a valid version (our assumption) , IS update its Active list by contact

RLSS and by the way update the Free list. MN will supply with those lists.

4. The MNs, WiFi APs, WhiteFi AP, and IS are MIH-capable nodes.
5. WiFi is considered as the preferred access network because, unlike WhiteFi, it works on unlicensed bands (without PUs) and has a higher throughput compared to WhiteFi.
6. The MN has a dual interface (WiFi–WhiteFi).
7. FMIPv6 is used as a mobility protocol.

4.5.5 System model

If the MN decides to connect with WhiteFi, we propose three schemes using TV channels classification which presented in section 4.5.4:

- **Scan all**

  Non-MIH-based case: MN must passively scan all 30 TVWS channels (ALL list). FMIPv6 should perform all its steps.

- **Scan free**

  MIH-based case: The Free list will scanned. Free list can be obtained from IS the every time the MN query IS. Free list updated at IS at least every 48 h (Figure 11-a). The Free list contains available channels, and it may contain the active ones. Even MIH is used here there is no improvement in the FMIPv6 delay, it should perform all its steps.

- **Scan active**

  An MIH-based case with RLSS: If MN has a Free list, this indicate the existing of WhiteFi around. To reduce Free list, MN sending MIH_Get_Information messages to IS querying only for WhiteFi to retrieve Active list, as shown in Figure 11-b, IS then contacts RLSS to retrieve the

Active list and Free list by the way. FMIPv6 time will reduce since the MD step is eliminated using IS information.

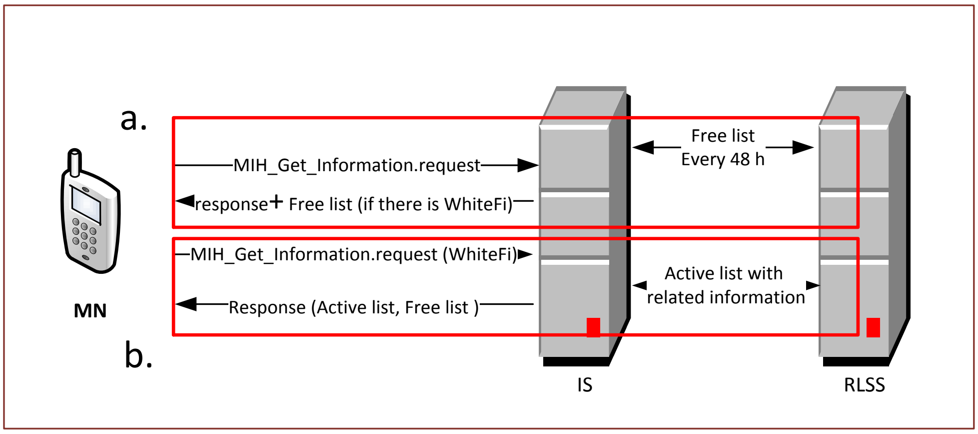

Figure 11. Proposed IS-RLSS integration

These three schemes are summarized in the following table, Table 5.

Table 5. Comparison of the Proposed Mechanisms

	Channels to scan	MIH	IS	RLSS	Updating IS	FMIPv6 Enhancement
Scan all	30	MIH not used				No
Scan free	Free list: Average 19 in rural	Yes (obtain Free list)	Yes, Before HO trigger	Yes, before HO trigger	At least every 48 h	No
Scan active	Less than "Free list"	Yes (obtain Active list)	Yes, after HO trigger	Yes, after HO trigger	On MN request	Yes

4.5.6 HO Signaling

This section presents the signaling messages of the three proposed mechanisms for HO from WiFi to WhiteFi.

1. *Signaling scheme of Scan all (without MIH)*

1. When MN moves to the edge of the WiFi cell, RSS will decrease and the Link_Going_Down trigger will be sent.
2. If there are no WiFi APs, the MN starts to passively scan 30 TVWS channels. If it finds one WhiteFi or more, the MN decides to which it will perform the HO.
3. FMIPv6 starts executing the HO operation. L2 HO starts as soon as it receives the FBAck message and all incoming data is forwarded to the NAR. After a successful L2 HO, FMIPv6 will complete its procedure and all buffered data will be forwarded to the MN.

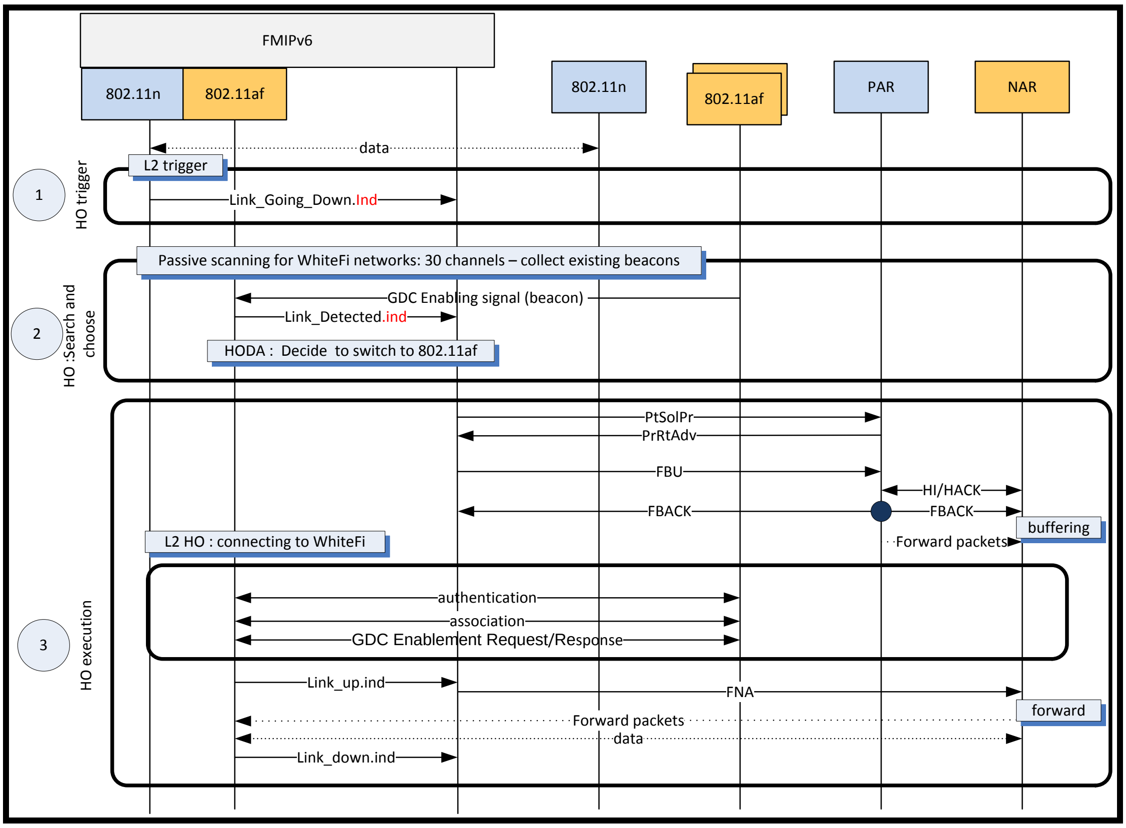

Figure 12. Scan all HO signaling

2. *Signaling scheme of Scan free (with MIH)*

0. At the point of initial contact between the MN and the WiFi, the MN connects with the IS to discover the area. The Free list is included if there is an existing WhiteFi AP and the list will be updated at MN every time it contact IS.
1. When the MN moves to the edge of the WiFi cell, RSS will decrease and the Link_Going_Down trigger will be sent. A MIH_Link_Going_Down will be sent to the upper layers to initiate HO.
2. The IS information is valid at MN and indicates no other WiFi APs in the area. Because information from IS contains Free list, it means there is a potential for existing WhiteFi APs. The MN starts to passively scan TVWS

free channels. If it finds one or more free channels, the MN decides to which it will perform the HO.

3. FMIPv6 starts executing the HO operation. L2 HO starts the moment it receives the FBAck message and all incoming data is forwarded to the NAR. After a successful L2 HO, FMIPv6 completes its procedure and all buffered data is forwarded to the MN.

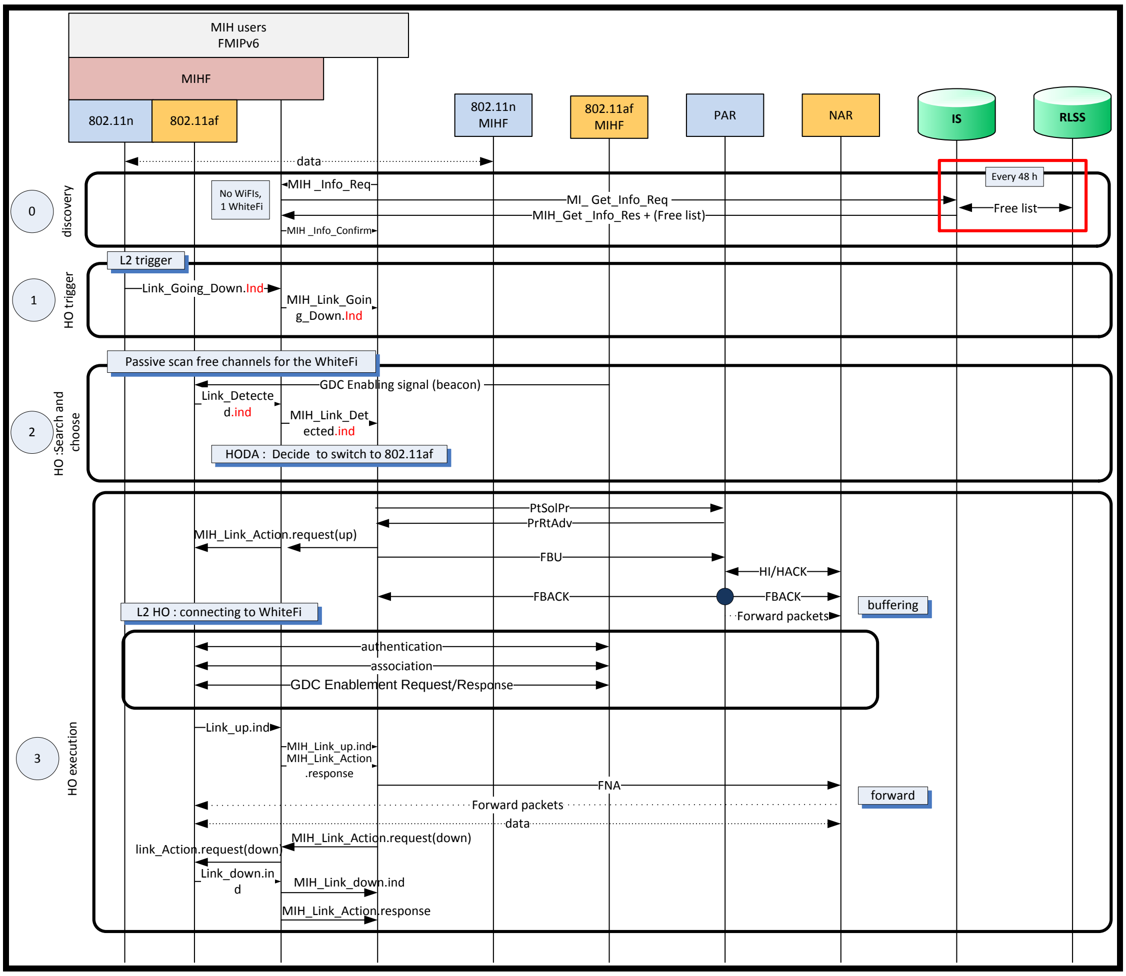

Figure 13. Scan free HO signaling

3. *Signaling scheme of Scan active (with MIH (IS contact RLSS))*

0. At the point of initial contact between the MN and the WiFi, the MN connects with the IS to discover the area. The Free list is included if there is

an existing WhiteFi AP and the list will be updated at MN every time it contact IS.

1. When the MN moves to the edge of the WiFi cell, RSS will decrease and the Link_Going_Down trigger will be sent. A MIH_Link_Going_Down will be sent to the upper layers to initiate HO.
2. The IS information is valid at MN and indicates no other WiFi APs in the area. Because the information from IS contains the Free list, it means there is a potential for an existing WhiteFi AP. The MN sends a request to IS to retrieve Active list from RLSS. The Free list will include for future used. Once this is received, the MN starts to passively scan only active channels. The MN then decides the target of HO.
3. FMIPv6 will start executing its operation, but without solicitation/advertisement messages because it uses the address of the target AP as the next router. L2 HO starts the moment it receives the FBAck message and all incoming data is forwarded to the NAR. After a successful L2 HO, FMIPv6 completes its procedure and all buffered data is forwarded to the MN.

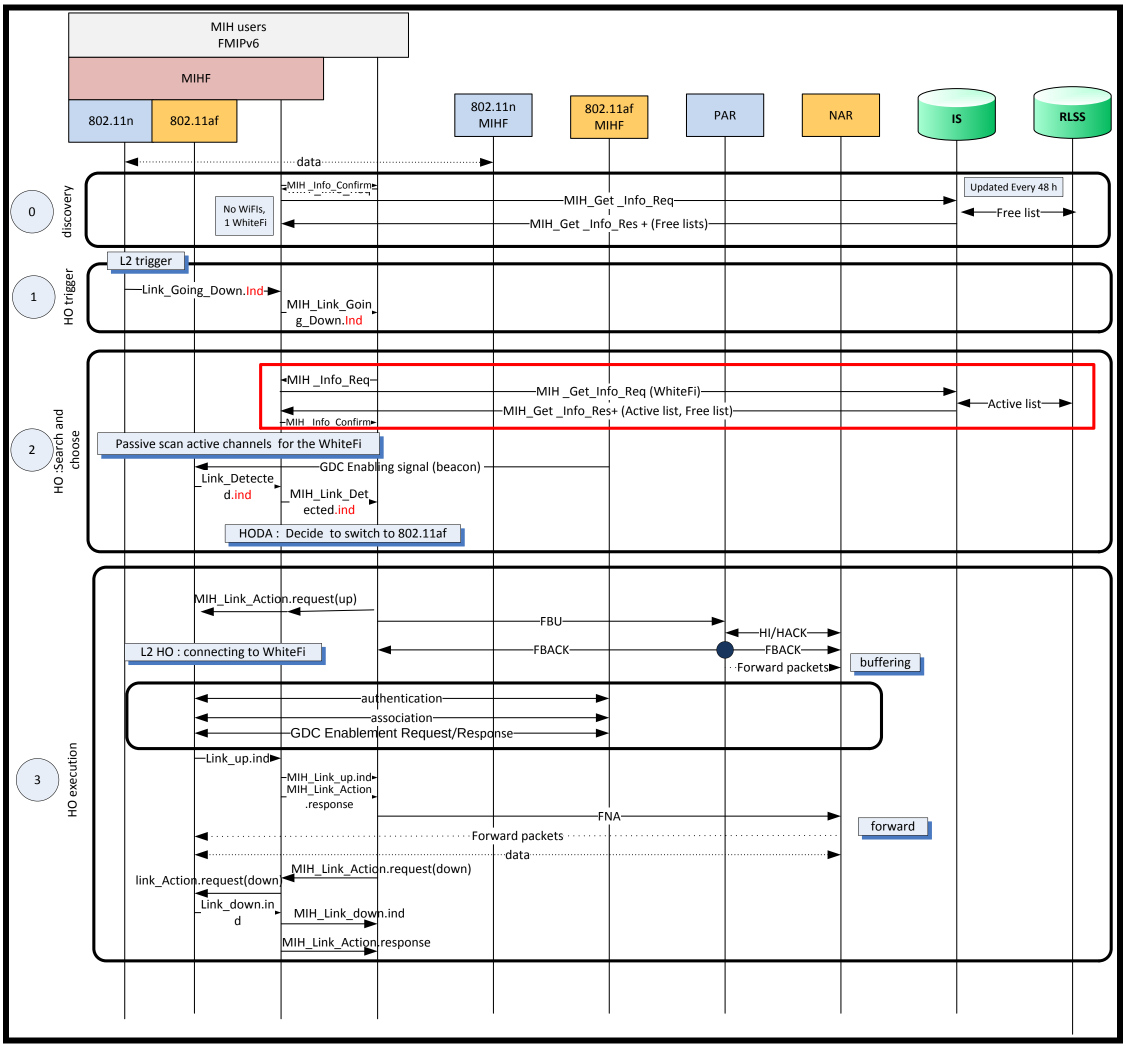

Figure 14. Scan active HO signaling

4.6 Total HO Delay Performance

To evaluate our model schemes, we compute the delay of each of the three schemes above. The length of the delay is one of the evaluation methods to measure the performance of HO; it is particularly relevant for our goal of reducing the scanning time. The following is our analytical model explanation. The symbols used in the formulas presented in this section are explained in Table 6 following the main three formulas of the schemes.

4.6.1 Total VHO delay

The HO process contains steps that include the decision to initiate HO, discovering the networks, choosing the target, and executing the HO. The total delay is the summation of the time needed to perform these steps, which can be expressed by the following formula.

$$\mathbf{T_{HO} = T_{decide\_to\_HO} + T_{scan} + T_{choose\_target} + T_{L2} + T_{L3},}$$

where $\mathbf{T_{HO}}$ is the total delay of HO, $\mathbf{T_{decide\_to\_HO}}$ is the time taken by MN to make a decision about triggering HO, $\mathbf{T_{scan}}$ is the time taken by MN to search for available networks, $\mathbf{T_{choose\_target}}$ is the time taken to decide the target AP, $\mathbf{T_{L2}}$ is the delay of the switch link at layer 2, and $\mathbf{T_{L3}}$ is the delay to perform L3 HO.

We can remove the "$\mathbf{T_{decide\_to\_HO}}$" and "$\mathbf{T_{choose\_target}}$" delays since they depend on the specific algorithms with varied delays (we consider the same HO decision and network selection schemes throughout the different schemes that we compare). The time of $\mathbf{T_{L2}}$ depends on the type of network. WhiteFi takes a little more time because it needs to perform the extra "enablement" procedure before establishing the link. The final base formula is

$$\mathbf{T_{HO} = T_{scan} + T_{L2} + T_{L3}.}$$

4.6.2 Scanning delay $\mathbf{T_{scan}}$

Scan all

According to the IEEE 802.11af standard, the MN cannot transmit on a TV channel unless it receives an enablement signal (beacon). Unlike normal WiFi, WhiteFi allow only to passively scan the TV channels to discover nearby APs. $\mathbf{D_P}$ is the total passive scan delay and calculated as:

$$\mathbf{T_{scan} = D_P(\mathit{m_1}) = \mathit{m}_1 * 0.1 \quad sec}$$

where $\boldsymbol{m_1}$ is the total number of channels (30 channels in case of WhiteFi) and the 0.1 sec represents the assumed beacon reception time (per channel).

$$\text{In WiFi, } \boldsymbol{m}_1 = 11 \text{ channels, meaning } \mathbf{D_P}=11*0.1=1.1 \text{ sec}$$

$$\text{In WhiteFi, } \boldsymbol{m_1} = 30 \text{ channels and } \mathbf{D_P} = 30 * 0.1 = 3 \text{ sec}$$

In WiFi, scanning time may take even less than 1.1 sec with active scan method while WhiteFi cannot.

Scan free - With MIH (IS)

We suppose that the IS, by contacting RLSS, provides the MN with the schedule of free channels (Free list, including active and non-active, and valid for 48 h). The MN scans all the channels in Free list, which is a subset of $\boldsymbol{m}_1$, $\boldsymbol{m_2}$.

$$0 \leq \boldsymbol{m_2} \leq \boldsymbol{m_1} \text{ channels}$$

$$0 \leq \mathbf{D_P}\ (\boldsymbol{m_2}) \leq 3 \text{ sec,}$$

where $\boldsymbol{m_2}$ is the subset list from TV channels ($\boldsymbol{m}_1$) and $\mathbf{D_P}$ $(\boldsymbol{m_2})$ is the total delay of scanning $\boldsymbol{m_2}$ channels. The MIH query IS after the MN attaches to the network periodically. Our assumption is that IS will include Free list with each query response. We assume that MN has a Free list and it is valid at time of HO trigger. The scan delay will calculate as:

$$\mathbf{T_{scan}} = \mathbf{D_P}\ (\boldsymbol{m_2}) = \boldsymbol{m_2} * 0.1 \quad \text{sec}$$

Scan active - With MIH (IS-RLSS)

When the IS contacts RLSS (responding to an MN request after HO trigger), it can provide the MN with specific WhiteFi APs with related (up to date) channels, Active list. The MN will only scan channels in the Active list, $\boldsymbol{m_3}$. $\boldsymbol{m_3}$ is the subset list from $\boldsymbol{m_2}$.

$$0 \leq \boldsymbol{m_3} \leq \boldsymbol{m_2} \text{ channels}$$

$$0 \leq \mathbf{D_P}\ (\boldsymbol{m_3}) \leq \mathbf{D_P}\ (\boldsymbol{m_2}),$$

where $\mathbf{D_P}$ $(\boldsymbol{m_3})$ is the delay of scanning active channels $\boldsymbol{m_3}$. To compute the actual time taken to scan the channels in this case, we should add two extra queries between MN and IS and between IS and RLSS, as follows:

$$\mathbf{T_{scan} = D_{IS\_Query} + D_{RLSS\_Query} + D_P}\ (\boldsymbol{m_3})$$

where $\mathbf{D_{IS\_Query}}$ is the delay of query IS and receives the response, and $\mathbf{D_{RLSS\_Query}}$ is the delay of query RLSS and receives the response. As a result, the scanning delay will be:

$$\mathbf{T_{scan}} = d_{IS\_query(MN \rightarrow IS)} + d_{IS\_query\ (IS \rightarrow MN)} + d_{RLSS\_query\ (IS \rightarrow RLSS)} + d_{RLSS\_query\ (RLSS \rightarrow IS)} + \boldsymbol{m_2} * 0.1$$

4.6.3 MAC layer (L2) HO delay

L2 HO consists of association and authentication (request/response) messages in WiFi. In WhiteFi, there is the need to exchange extra enablement (request/response) messages.

$$\mathbf{T_{L2\ (WiFi)} = D_{ass} + D_{auth},}$$

where $\mathbf{T_{L2\ (WiFi)}}$ is a L2 HO delay of WiFi, $\mathbf{D_{ass}}$ is the association delay, and $\mathbf{D_{auth}}$ is the authentication delay. $\mathbf{D_{ass}}$ and $\mathbf{D_{auth}}$ are exchanged between the MN and the NAP. At the end, the scanning delay is calculated as:

$$\mathbf{T_{L2\ (WiFi)}} = d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth\ (MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)}$$

To compute $\mathbf{T_{L2\ (WhiteFi),}}$ the enablement request/response messages delay $\mathbf{D_{enable}}$ will add:

$$\mathbf{T_{L2\ (WhiteFi)} = D_{enable} + D_{ass} + D_{auth}}$$

Enablement messages will also be exchanged between the MN and the NAP.

$$T_{L2\ (WhiteFi)} = d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable(MN \rightarrow NAP)} + d_{denable\ (NAP \rightarrow MN)}$$

4.6.4 Network layer HO delay

Scan all: MIH not used

In FMIPv6, the total delay can be calculated as:

$$T_{L3} = D_{MD} + D_{DAD} + D_{FNA},$$

where D_{MD} is the MD delay, MD process consisting of solicitation/advertisement messages exchanged between MN and PAR. D_{DAD} is the delay of DAD process. DAD is the process of creating CoA and validating it. The DAD consists of FBU/FBACK messages between MN and PAR and HI/HACK messages between PAR and NAR. The D_{FNA} is the advertisement message to indicate completion of L3 HO and to indicate that buffering data can be forwarded to the MN between the MN and the NAR.

$$T_{L3} = d_{RtSolPt(MN \rightarrow PAP)} + d_{PtRtadv(PAP \rightarrow MN)} + d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

Scan free: MIH used but without current connection with RLSS

The delay is still the same since we only have information about the free channels without any indication about the AP address.

$$T_{L3} = D_{MD} + D_{DAD} + D_{FNA}$$

$$T_{L3} = d_{RtSolPt(MN \rightarrow PAP)} + d_{PtRtadv(PAP \rightarrow MN)} + d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

Scan active: With MIH with current connection with RLSS

$\mathbf{D_{MD}}$ will be removed because the MN can obtain information from the HO trigger.

$$\mathbf{T_{L3} = D_{DAD} + D_{FNA}}$$

$$\mathbf{T_{L3}} = d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

As a result, the total delays for each of the proposed scenarios are

$$\mathbf{T_{HO} = T_{scan} + T_{L2} + T_{L3}}$$

$$\mathbf{T_{HO\_scan\_all}} = \boldsymbol{m_1} * 0.1 + d_{RtSolPt(MN \rightarrow PAP)} + d_{PtRtadv(PAP \rightarrow MS)} + d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable\ (MN \rightarrow NAP)} + d_{enable\ (NAP \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

$$\mathbf{T_{HO\_scan\_free}} = \boldsymbol{m_2} * 0.1 + d_{RtSolPt(MN \rightarrow PAP)} + d_{PtRtadv(PAP \rightarrow MS)} + d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable\ (MN \rightarrow NAP)} + d_{enable\ (NAP \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

$$\mathbf{T_{HO\_scan\_active}} = d_{IS\text{-}query\ (MN \rightarrow IS)} + d_{IS\text{-}query\ (IS \rightarrow MN)} + d_{RLSS\text{-}query\ (IS \rightarrow RLSS)} + d_{RLSS \rightarrow query\ (RLSS \rightarrow IS)} + \boldsymbol{m_3} * 0.1 + d_{FBU(MS \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MS)} + d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable\ (MN \rightarrow NAP)} + d_{enable(NAP \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

Table 6. Descriptions of Equation Symbols

Symbol	Description	Symbol	Description
MN	Mobile Node	$d_{PtRtadv}$	Delay for advertisement message
IS	Information Server	d_{FBU}	Delay for FBU message
RLSS	Registered Location Secure Server	d_{HI}	Delay for HO Initiation message
PAR	Previous Access Router	d_{HACK}	Delay for HO Acknowledgment message
NAR	New Access Router	d_{FBACK}	Delay for Fast Binding Acknowledgment message
PAP	Previous AP	d_{FNA}	Delay for Neighbor Advertisement
NAP	New AP	$d_{IS\text{-}query}$	Delay for MIH_Get_Information message
$D_P(m_1)$	Passive scan delay for all channels: m_1=30	$d_{RLSS\text{-}query}$	Delay for New IS_RLSS message
$D_P(m_2)$	Passive scan delay for free channels: m_2	d_{enable}	Delay for enablement request/response message
$D_P(m_3)$	Passive scan delay for active channels: m_3	d_{ass}	Delay for association request/response message
$d_{RtSolPt}$	Delay for solicitation message	d_{auth}	Delay for authentication request/response message

4.6.5 Delay calculation

The delay of a single message is defined as "how long it takes for an entire message to completely arrive at the destination counting from the first bit that is sent out from the source"[40].

Delay = propagation time+ transmission time + queuing time + processing time

To calculate a delay for a single message moving from two nodes, we sum four components:

- **Propagation Delay**: time required for a bit to travel from the source to the destination (P).

  Propagation Delay = Distance m / Propagation speed m/sec = $\frac{d}{Pr}$ sec

- **Transmission Delay**: time between the first bit leaving the sender and the last bit arriving at the receiver.

  Transmission Delay = message size bit / bandwidth bit /sec = $\frac{S}{B}$ sec

- **Queuing Delay** [41]: the required time for each intermediate or end device to hold the message before it can be processed.

  We consider **M/M/1** Queueing model where the packet arrival and service rate distribution are both Poisson with rates **λ** and **μ**, respectively. The mean packet delay is **1/ (μ - λ). μ** is calculated by dividing the average packet size (**m**) with the link transmission capacity (**B**); therefore, we have:

  $$\text{Queuing delay}= \frac{m}{B- m\lambda}$$

- **Processing Delay**: the time it takes the routers to process the packet header, P_d.

4.6.6 Calculation for each message

Each message travels across different nodes via a number of wired and/or wireless media. We consider the number of hops that each message will cover between source and destination. We denote the numbers of hops as $h_{x \rightarrow y}$, where ***x*** is the source of the messages and ***y*** is the destination. We can redefine the equation above for each message considering the numbers of hops, as follows:

- **Transmission Delay and Propagation Delay**

  We can add the propagation delay to the transmission time, as in [42]:

  $$\text{Transmission delay} = \frac{S}{B} + P$$

  Thus, the delay for a message crosses different nodes:

  $$\textbf{Transmission delay} = \frac{S}{Bwl} + P_{wl} + h_{x \rightarrow y} \times (\frac{S}{Bw} + P_{w}),$$

  where ***S*** is a message size, ***Bw*** and ***Pw*** are the bandwidth and propagation delay of wired media, respectively, and ***Bwl*** and ***Pwl*** are the bandwidth and propagation delay of wireless media, respectively.

- **Queuing delay** $= \frac{m}{Bwl - m\lambda} + \sum_{k=1}^{n} (\frac{m}{Bw - m\lambda}),$

  where *n* is the number of hops.

- **Processing delay** $= (h_{x \rightarrow y} + 1) \times P_d$

Signaling Message Delay = transmission time + queuing time+ processing time

di(x->y) =T +Q +P,

where ***i*** is the message name, ***x*** is the source of the message, and ***y*** is the destination of the message. Note that, when the message is not related to the MN as source or destination, the wireless related part in the equations should be removed.

4.6.7 Parameters

Table 10 shows the parameters with the values used in the calculations. The parameter values assumed in the calculations were taken from [28] for FMIP messages and from “RFC 5677” for MIH messages. “RFC 5677” gives a size range starting from 30 bytes to 65,000 bytes for MIH_Get_Information message. We assumed a minimum size for request and a maximum size for response. For new message Query_RLSS request/response, we assumed that its size is the same as that of MIH_GET_Information, since they ,by our assumptions, hold same information. Concerning the enablement request/response messages, the respective values were taken from standards. Other values such as Pd and Bw were based on [42]. The following tables contain all the values used in our analytical model.

Table 7. FMIP Signaling Message Size and Relative Distance in Hops

FMIP Messages	Size in Bytes	Source (x)	Destination (y)	No. of hops from x to y ($h_{x \to y}$)
Rt. Solic.	52	MN	PAR	1
Rt. Adv.	80	PAR	MN	1
FBU	56	MN	PAR	1
HI	52	PAR	NAR	1
HACK	52	NAR	PAR	1
FBACK	56	PAR	MN	1
FNA	52	MN	NAR	2

Table 8. MIH Signaling Message Size and Relative Distance in Hops

MIH Messages	Size in Bytes	Source (x)	Destination (y)	No. of hops from x to y ($h_{x \rightarrow y}$)
MIH_Get_Info.Request	30	MN	IS	2
MIH_Get_Info.Response	65,000	IS	MN	2
NEW Query_RLSS.Request	30	IS	RLSS	1
NEW Query_RLSS.Response	65,000	RLSS	IS	1

Table 9. L2 (802.11) Signaling Message Size 1 and Relative Distance in Hops

Message	Size in Byte	Source (x)	Destinatio n (y)	No. of hops from x to y ($h_{x \rightarrow y}$)
Enablement Request	40	MN	NAP	0
Enablement Response	63	NAP	MN	0
Authentication Request	30	MN	NAP	0
Authentication Response	30	NAP	MN	0
Association Request	44	MN	NAP	0
Association Response	52	NAP	MN	0

[1] http://web.cecs.pdx.edu/~jrb/netsec/lectures/80211/associate.txt

Table 10. Parameter Descriptions and Values

Parameter	Description	Value
B_{wl}	Bandwidth of wireless link.	WiFi <= 300 Mbps WhiteFi 12 Mbps
B_w	Bandwidth of wired link.	100 Mbps
P_{wl}	propagation delay of the wireless link	WiFi = .0005 ms WhiteFi = .0016 ms
P_w	propagation delay of the wired link	0.5 ms
$h_{x \rightarrow y}$	Distance in hops	Tables 7,8,9
s	Massage size	Tables 7,8,9
λ	Arrival rate at network node	10-1,000 packets
m	Mean packet size distribution	454 bytes
P_d	Processing delay at node	0.001 sec

4.7 Conclusion

In this chapter, we proposed an IS-RLSS interworking for WiFi/WhiteFi integrated networks with a HO scanning mechanism using MIH and FMIPv6 protocols in order to perform HO with minimal delay. With the help of MIH, the MN can communicate with the IS to hold the information about neighboring networks. We assumed that this server can access RLSS, which is a server that contains only WhiteFi channel availability information, to extract both Free list channels and Active list channels with the respective association information. The analytical model and data provided in this chapter are used in the following chapter to evaluate and analyze the performance of the proposed technique by comparing it with the baseline case in which MIH is not used.

Chapter 5

Results

5.1 Introduction

Based on the analytical model and parameters presented in Chapter 4, this chapter presents results of the proposed HO schemes between WiFi and WhiteFi networks. The results of the HO delay for the three proposed techniques are presented and compared. The HO delay behavior is studied against the variation of the following parameters: throughput, number of MNs, number of hops, and number of HO requests at the RLSS. Finally, the end of this chapter presents a summary of the findings of these numerical results.

5.2 WiFi to WhiteFi HO Total Delay

In the proposed model, the HO Delay is considered the time difference between the moment when the MN decides to HO until the L3 HO is finished. The delay is counted after the L2 trigger when the MN starts to scan for new APs until the NAR receives an FNA acknowledgement from the MN indicating that it can forward the buffered data. The delay is an important factor in evaluating any HO solution, as it specifies the reliability of that approach. When the HO delay is high, the connection with the serving network might be lost before completing its connection with the target network. In our case, the scan time takes up most of the HO processing time.

The total HO delay is computed as a summation of the delay for all messages exchanged during the HO process. The delay of a single message will be calculated from the equations presented in the previous chapter, for each case in the proposed work. The HO delay equations for all three cases are listed below:

Base case: Scan All, without MIH protocol.

$$\boldsymbol{m_1} * 0.1 + d_{RtSolPt(MN \rightarrow PAP)} + d_{PtRtadv(PAP \rightarrow MS)} + d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable\ (MN \rightarrow NAP)} + d_{enable\ (NAP \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

Enhanced case 1: Scan Free, with MIH protocol: partial information (Free list).

$$\boldsymbol{m_2} * 0.1 + d_{RtSolPt(MN \rightarrow PAP)} + d_{PtRtadv(PAP \rightarrow MS)} + d_{FBU(MN \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MN)} + d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable\ (MN \rightarrow NAP)} + d_{enable\ (NAP \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

Enhanced case 2: Scan Active, with MIH protocol + RLSS: full WhiteFi APs information (Active list).

$$d_{IS\text{-}query\ (MN \rightarrow IS)} + d_{IS\text{-}query\ (IS \rightarrow MN)} + d_{RLSS\text{-}query\ (IS \rightarrow RLSS)} + d_{RLSS \rightarrow query\ (RLSS \rightarrow IS)} + \boldsymbol{m_3} * 0.1 + d_{FBU(MS \rightarrow PAR)} + d_{HI(PAR \rightarrow NAR)} + d_{HACK(NAR \rightarrow PAR)} + d_{FBACK(PAR \rightarrow MS)} + d_{ass\ (MN \rightarrow NAP)} + d_{ass\ (NAP \rightarrow MN)} + d_{auth(MN \rightarrow NAP)} + d_{auth\ (NAP \rightarrow MN)} + d_{enable\ (MN \rightarrow NAP)} + d_{enable(NAP \rightarrow MN)} + d_{FNA(MN \rightarrow NAR)}$$

Using the parameters presented in Chapter 4, the HO delay from WiFi to WhiteFi is equal to 3.026 seconds for the first case (Scan all) listed above with scanning 30 channels. According to the percentages presented in Chapter 2, the actual average number of TVWS channels available to connect to portable devices is 61.8% and 32.1% for rural and urban environments, respectively. The delay in the second case (Scan free) is 1.926 seconds for rural environments, while for urban, it should be less since there are less free channels. The channels in the Active list will be less or equal to the Free list in the worst case. For the third case (Scan active), the total delay varied from 0.149 to 1.949 seconds, when we assumed that active channels ranged from 1 to 19 channels. Figure 15 shows the comparison between the three schemes and displays all possible cases for the third (Scan active) case.

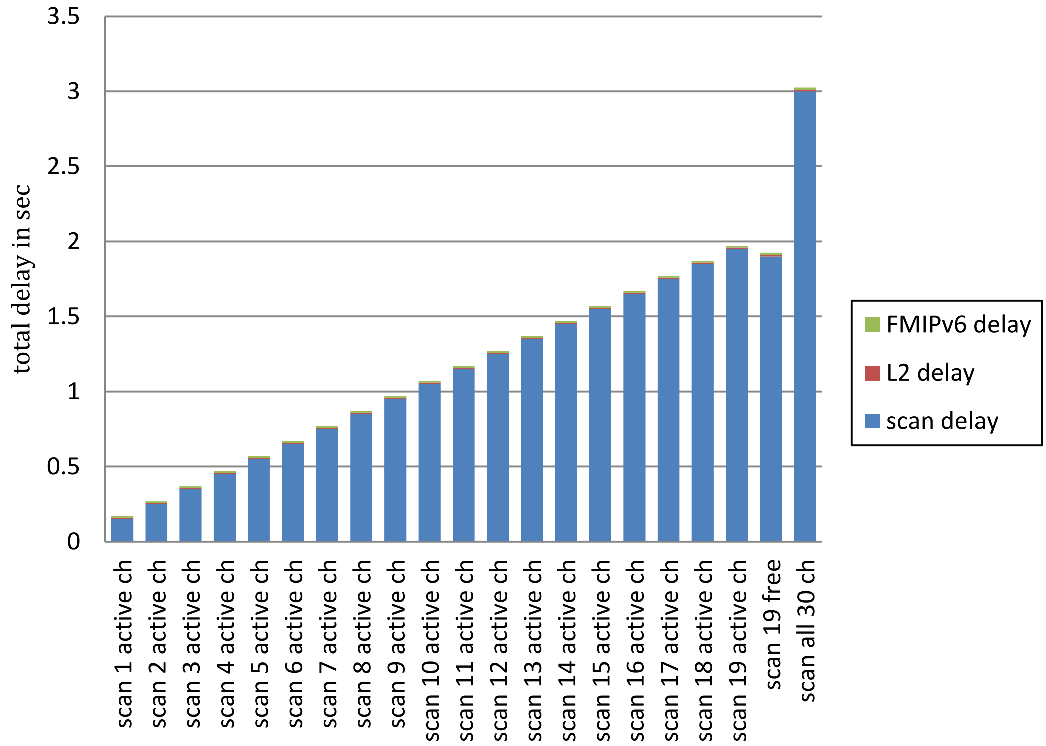

Figure 15. Comparison of HO total delay for the three schemes

In the next four sections, we examine the variation of the total HO delay against the change of various parameters such as throughput, number of MNs, number of hops to reach IS, and number of requests at IS.

5.2.1 Behavior of HO delay against WiFi link throughput

The throughput of WiFi is considered to be 300 Mbps, as an assumption in our model, and this is the maximum value with 20 MHz as in the standard. We also assumed lower throughput values to represent suboptimal cases. The test values consist of 1 Mbps, 11 Mbps, 54 Mbps, 100 Mbps, and 300 Mbps. The processing delay for each message delay was not considered since it did not depend on the WiFi throughput. The arrival rate was fixed to 10 packets per second in this test. The number of active and free channels does not affect the result since the scanning delay was removed. The result is shown in Figure 16 for selected values of active channels and in Figure 17 for all possible values of active channels ≤ 19.

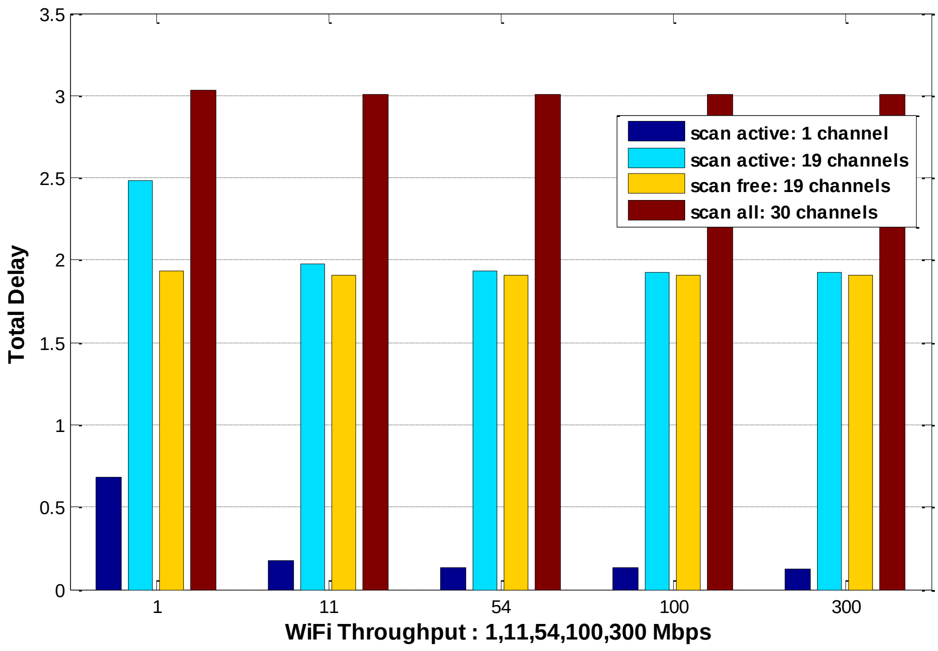

Figure 16 Total HO delay (sec) vs. WiFi throughput

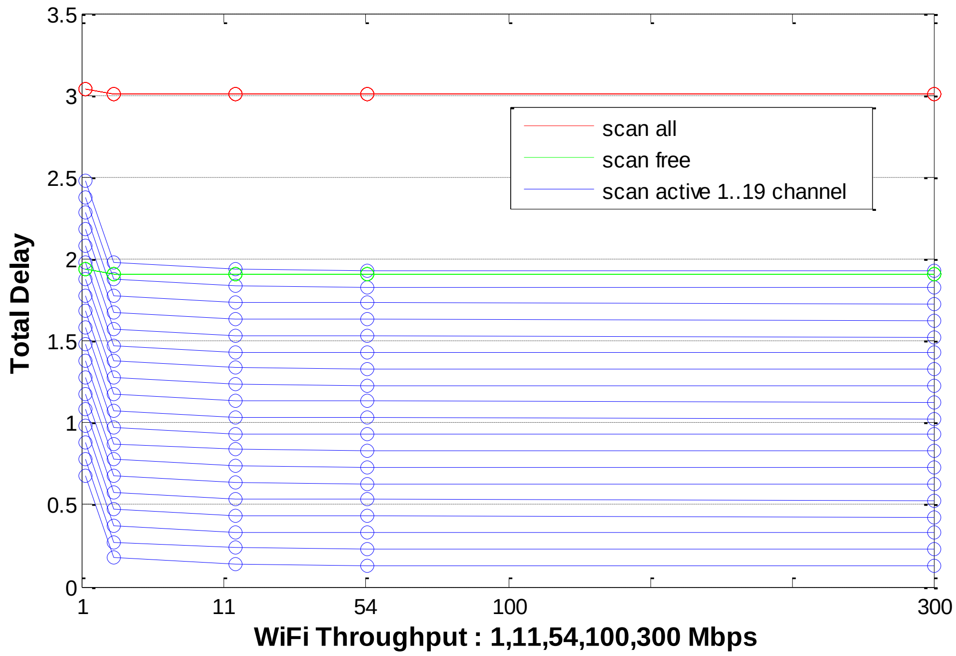

Figure 17. Total HO delay (sec) vs. WiFi throughput

The big throughput effect is on Scan active. Scan all and Scan free take the same delay since they have same messages (the difference will be in the scanning delay since they have different number of channels to scan). By increasing the throughput, the delay was considerably reduced by 500 ms at 11 Mbps. The advantages of increasing throughput disappear after 54 Mbps and the delay begins to equalize. With 1 Mbps, scanning more than 13 channels caused a longer delay than in the case of Scan free with 19 channels but with 11 Mbps and other throughput values only 19 channels in Scan active have a greater delay than Scan free.

5.2.2 Behavior of HO delay against the number of MNs

Based on the same circumstances as section 5.2.1, we studied the delay which results from changing the number of MNs with throughput equal to 300 Mbps. As shown in

Figure 18, an increasing number of MNs in the serving network leads to an increased delay in the HO. Scan active is most affected by decreased throughput. Scan all and Scan free are unnoticeable changes by the increasing number of MNs.

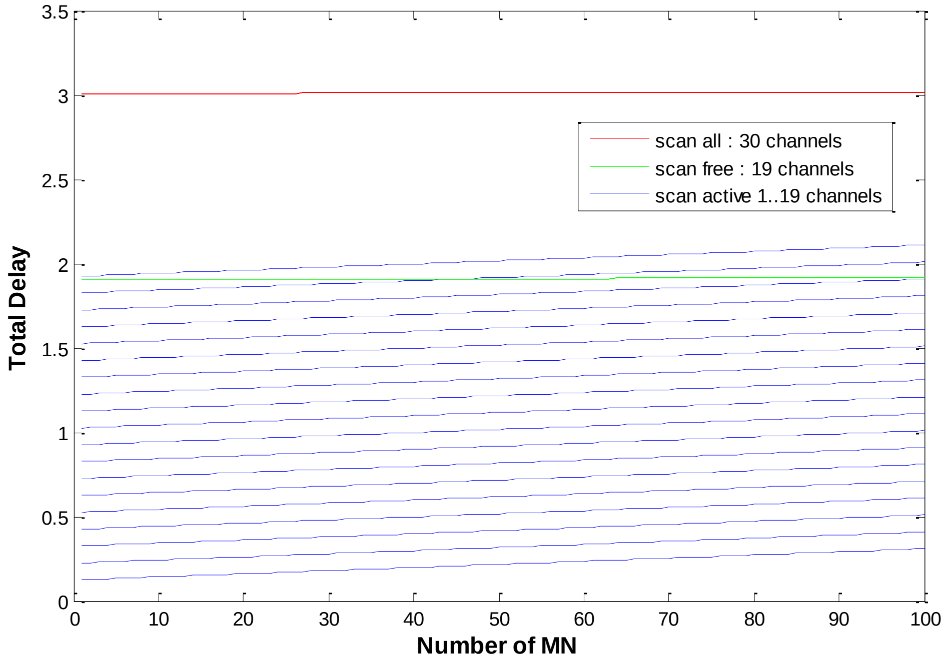

Figure 18. Total HO delay (sec) vs. number of MNs

5.2.3 Behavior of HO delay against distance to RLSS (Scan active)

The proposed Scan free and Scan active schemes reduce the scanning time by reducing the number of channels to be scanned. As Scan active obtains the subset of Free list, the delay reduces because it retrieves only those channels used by APs and this is vary go to zero in the case when no WhiteFi AP available in the area. The good result obtained by the Scan active scheme is because the IS sends queries to RLSS to retrieve Active list contains active channels with relative information. This means extra messages are exchanged between the MN and RLSS. In this section, we study the effect of the variable distance from RLSS to IS on the overall HO delay for Scan active. The increasing number of nodes between IS and RLSS or between MN and IS will be effect the delay of Query_RLSS anc I_Get_info request/response messages. However, we do not study increasing of path between other nodes because even if they are affected the delay, but with the same effect on all three schemes. In this section we focus on IS and RLSS path where variable distance value starts at two and continues until it reaches 255. The value of $h_{x \rightarrow y}$ is the distance in hops between the source and destination of the message. The number of hops that the MN should pass before reaching the destination is called time to live (TTL). It is a field in the packet header; 255 is the maximum, which indicates the packet was lost.

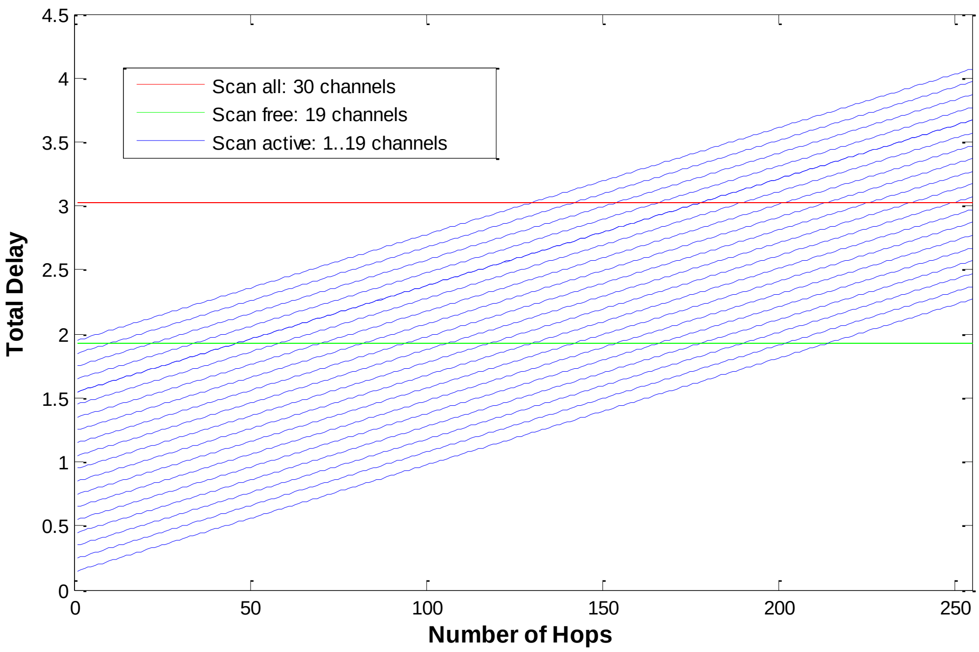

Figure 19. HO delay (sec) vs. distance in hops to RLSS

In the best case in Scan active, where the number of active channels is equal to one, with an increasing number of hops between MN and RLSS, the delay increases. We increase the numbers of hops until the delay exceeds the delay of Scan all. However, the delay in Scan active with one active channel does not exceed Scan all and more than 200 hops are required to exceed the delay of Scan free. If there are 19 channels in the Active list and MN chooses to scan all of them, the delay is already more than that of Scan free with 19 free channels, but 130 nodes are needed for the delay to be longer than Scan all.

5.2.4 Behavior of VHO latency against RLSS request rate (Scan active)

This section shows the HO delay for Scan active approaches with respect to the variable HO query requests arrival rate on RLSS. RLSS does not play any role in the Scan all and Scan free schemes. The HO query requests variation at RLSS based on the following equation, since RLSS as a server connects with a wired link:

$$q_{w=}\frac{m}{Bw- m\lambda}$$

where ***Bw*** is wired throughput, ***m*** is mean packet size, and $\boldsymbol{\lambda}$ is the request arrival rate. $\boldsymbol{\lambda}$ will vary until $\boldsymbol{m\lambda}$ reaches the close limit of the wired link throughput (100 Mbps) in the query message, only at RLSS. For the rest of the messages including the RLSS request messages when pass on other nodes, **λ**=10. Transmission, processing, and scanning delays are eliminated for this test. The mean packet size ($\boldsymbol{m}$) takes low and high values.

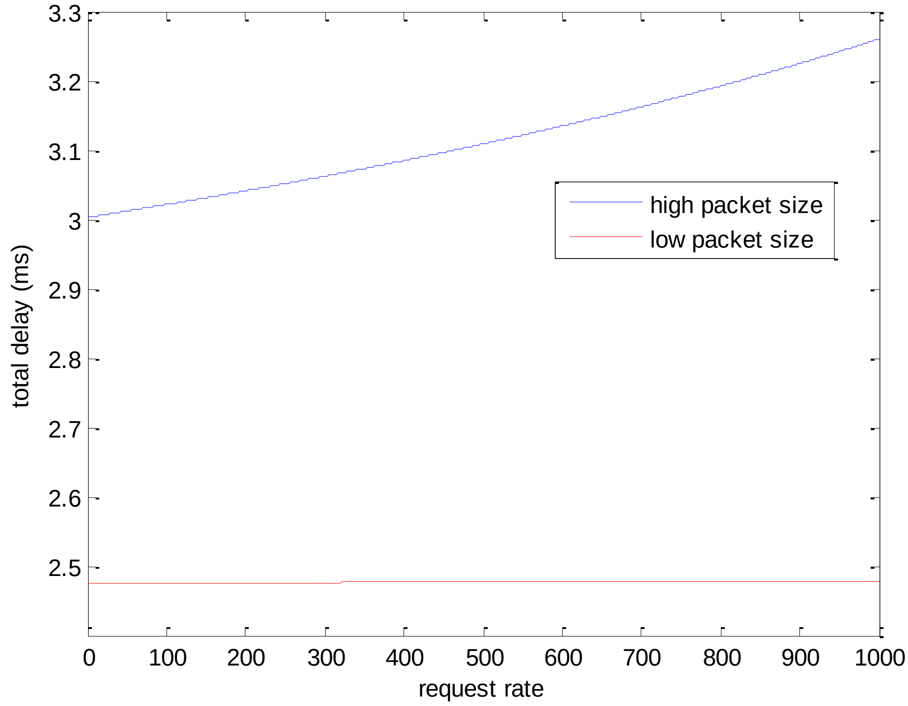

Figure 20. Queuing delay (ms) vs. request rate

Figure 20 shows how the HO delay is affected by the increasing HO query requests on RLSS for Scan active regardless of scanning time. The difference is small and the total HO delay is not significantly affected since queuing delay is a small part of it. The delay starts changing rapidly after 26,000 requests, as shown in Figure 21, since 27,250 is the maximum theoretical request rate that we extract from the queuing delay equation in the case of a small mean packet size.

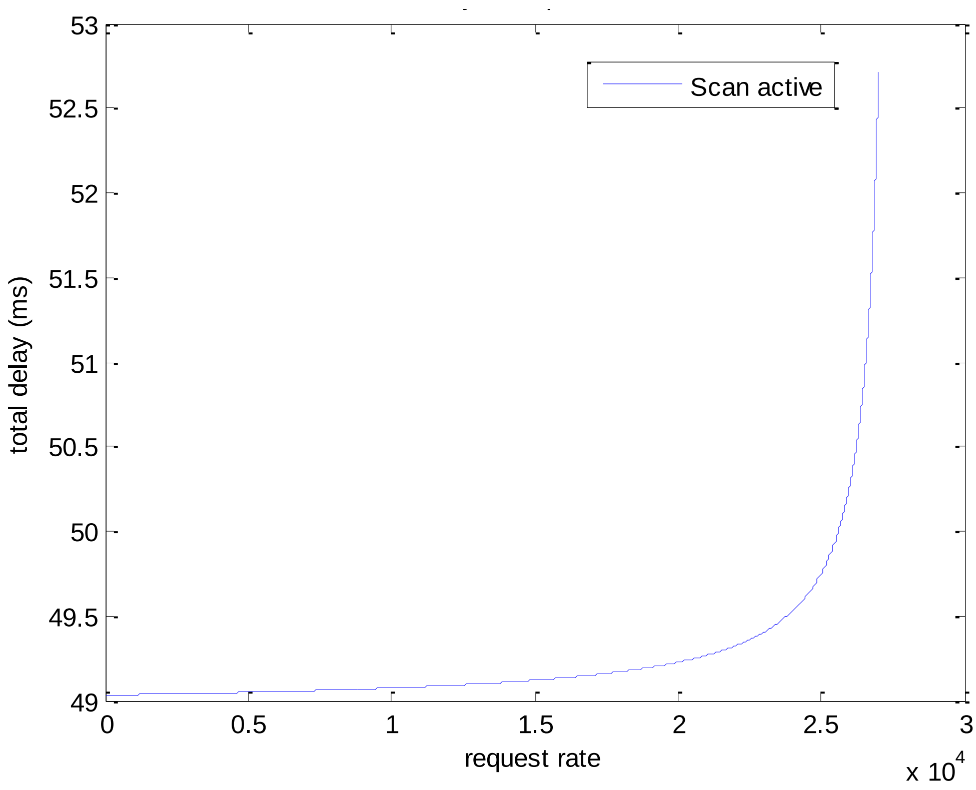

Figure 21. Queuing delay (ms) vs. request rate

5.2.5 Behavior of VHO latency against RLSS/IS response message size

In all calculations through this thesis we assume that the size of MIH_Get_Info and Query_RLSS responses messages is equal to 65000 bytes for each while for respective requests the size is equal to 30 bytes. In the Scan all mechanism, the MN will query only resources for the WhiteFi network. In the MIH protocol, the MN can specify the networks that it is looking for as well as the size limit of response message. In the results the size of the response message could be less than 65000 bytes. Here we study the effect of decreasing the size of MIH_Get_info and Query_RLSS messages on the total HO delay for the Scan active approach. We assume that the same content will be included in both messages so they have same size. Different indicative sizes (65000, 20000, 5000, 2000) for each message are studied. Table 11 shows the approximate values of the delay of these two separate messages and the total delay of HO without including the scanning delay. Also this Table represent the percentage of the enhancement. Figure 22 shows the total HO values that are included in the table. From the table we can see that when decreasing the size, the delay will be reduced at steady rate. We also calculated the percentage of enhancement for total HO delay including scanning time with some selected channels number (1, 10, 19, 30) and the results are show in Table 12 and Figure 23. For example, the delay of those two messages reduced by 34% when we decreased the size by 45000 bytes. When we included the scanning delay the enhancement dropped to 8%, 1.17%, 0.63%, and 0.40% assuming that we scanned 1, 10, 19, and 30 channels respectively. We can conclude that the enhancement will be of the order of 1% each time we reduce the message size by each 5600 bytes. This percentage will be reduced when including scanning delay as seen in Table 12.

Table 11 The delay of MIH_Get_Info and Query_RLSS response in Scan active for different messages size

Size in bytes	MIH_Get_info response delay in sec	Query_RLSS response delay in sec	Delay of both messages in sec	Enhancement of the messages delay	Total HO delay (without scanning delay)	Enhancement of the total HO delay (without scanning delay)
65000	0.016	0.007	0.023	---	0.0494	---
20000	0.008	0.007	0.015	34%	0.0371	24%
5000	0.005	0.007	0.012	47%	0.0335	32%
2000	0.005	0.002	0.007	69%	0.0326	34%

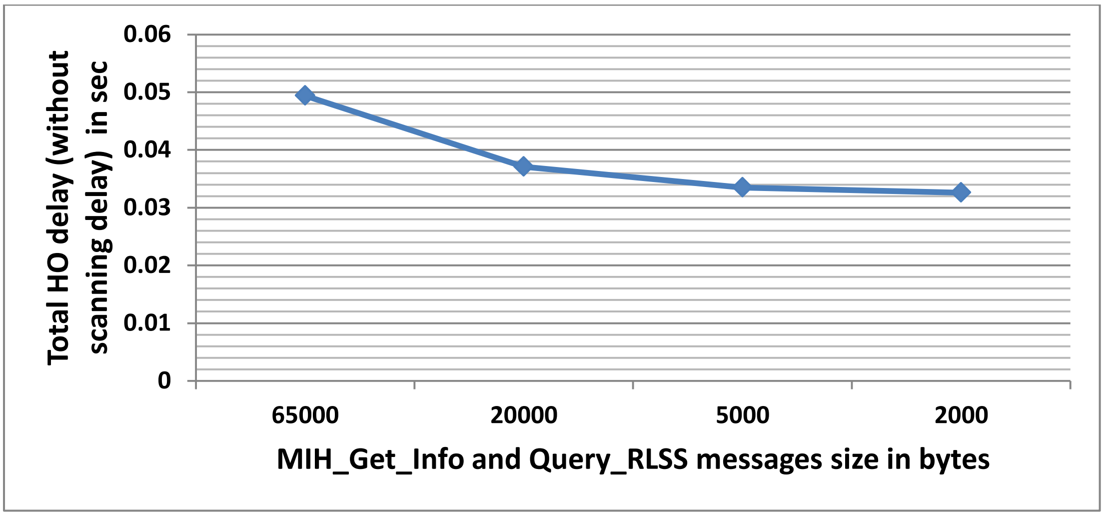

Figure 22 The delay of MIH_Get_Info and Query_RLSS response in Scan active vs messages size

Table 12 The total HO delay of "Scan active" with 19,30 active channels for diffrent MIH_Get_Info and Query_RLSS response messages size

	Enhancement of the "Scan active" total HO delay include the delay of scanning 0,1,19,30:				
Messages size	No scanning delay	1 active channel	10 active channel	19 active channels	30 active channels
65000	-----	---	---	---	---
20000	24%	8%	1.17%	0.63%	0.40%
5000	32%	10.6%	1.52%	0.82%	0.52%
2000	34%	11%	1.60%	0.86%	0.55%

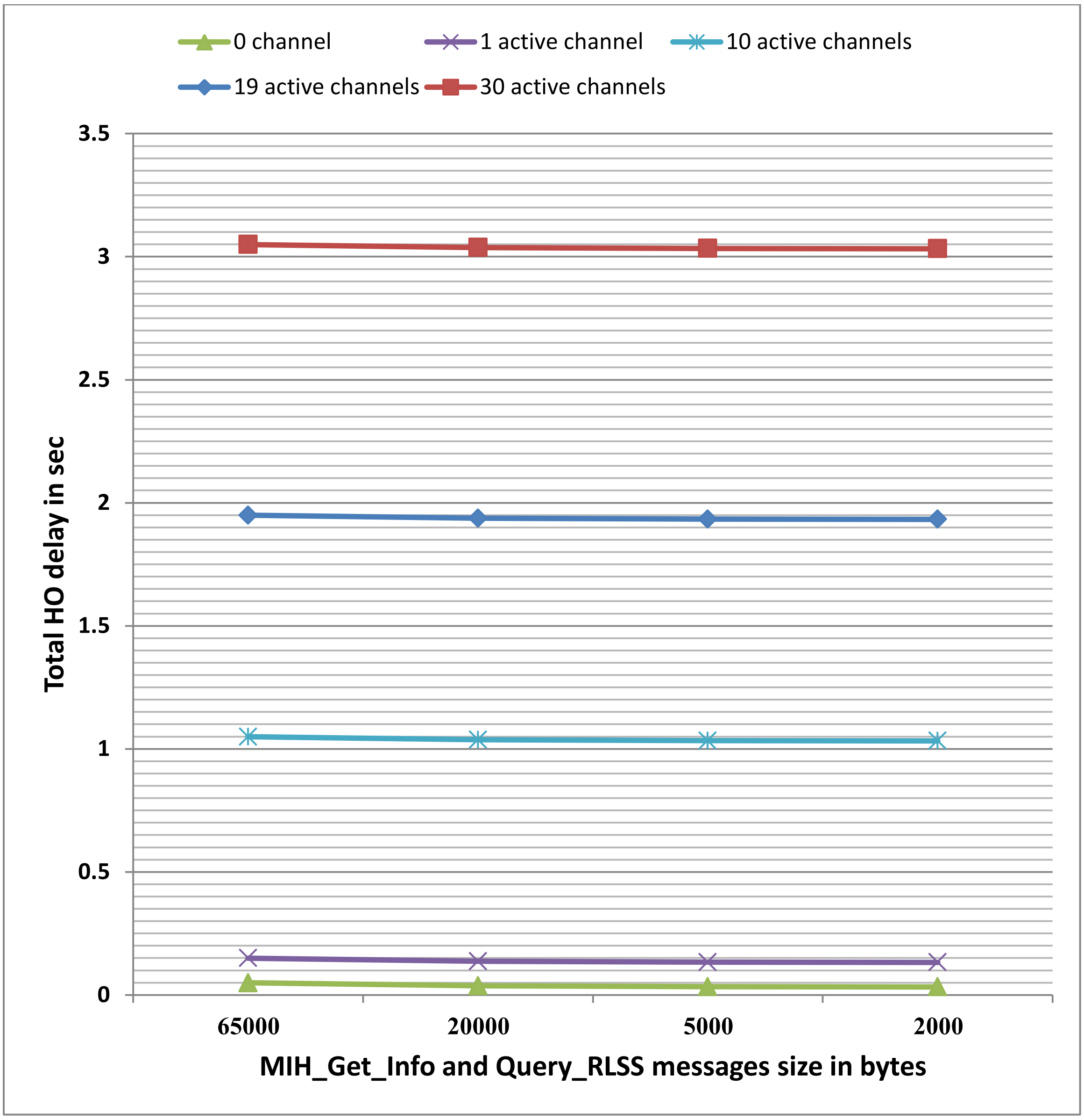

Figure 23 The total HO delay of "Scan active" with 19,30 active channels for diffrent MIH_Get_Info and Query_RLSS response messages size

5.3 Conclusion

The performance of the proposed HO schemes is tested in terms of HO total delay including scanning and pre-scanning phases, which start after HO is triggered. This delay is affected by changes in the values of its parameters. This chapter studied the behavior of total HO delay against throughput, number of MNs, number of hops to reach RLSS, the number of request at RLSS, and the size of MIH_Get_Info and Query_RLSS response messages. The results show the varying effects of these parameters on the three proposed schemes. The next chapter aims to explain this variation.

Chapter 6

Discussion

6.1 Introduction

Chapter 5 studied the total delay of HO for three proposed schemes. In separate sections, we showed how the behavior of total delay changes with varying throughput, number of MNs, request rate, and number of hops. In this chapter, the reasons why some parameters have greater effects on the result than others will be discussed. Other numerical results and analyses will be presented.

6.2 HO Total Delay

By dividing the delay into three components of scanning, L2 HO, and L3 HO delays for a Scan active case with one active channel (Figure 24), it is clear that the scanning time causes most of the delay. This difference increases as the number of active channels increases.

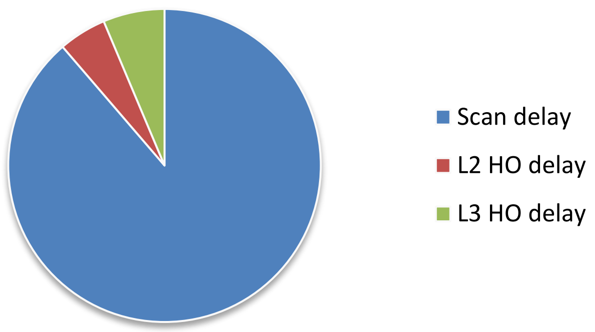

Figure 24. HO delay of different phases of scan active with one active channel

6.3 Analysis of Total Delay Behavior

The delay for each message consists of transmission, processing, and queuing delays. As the delay comes from L2 and L3 HO messages and querying IS in the third scheme ,Scan active, Figures 25 and 26 show how these three core message delay components affect each scheme (only for messages, eliminating scanning delay).

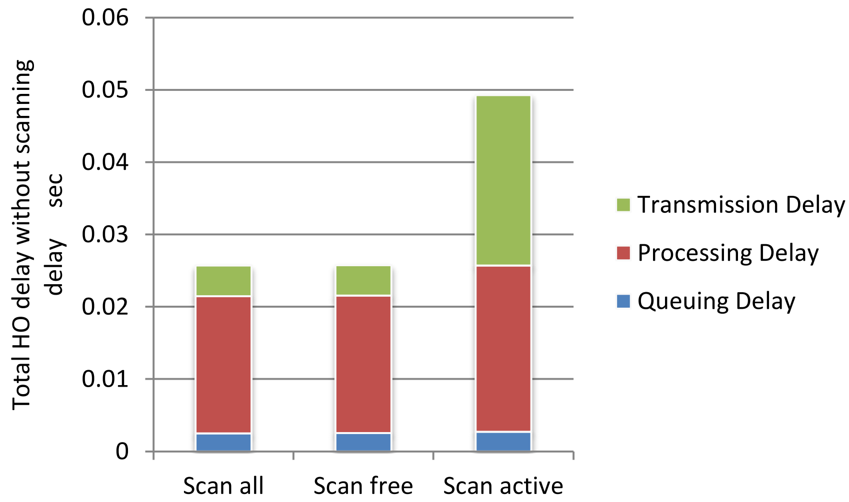

Figure 25. Components of total delay

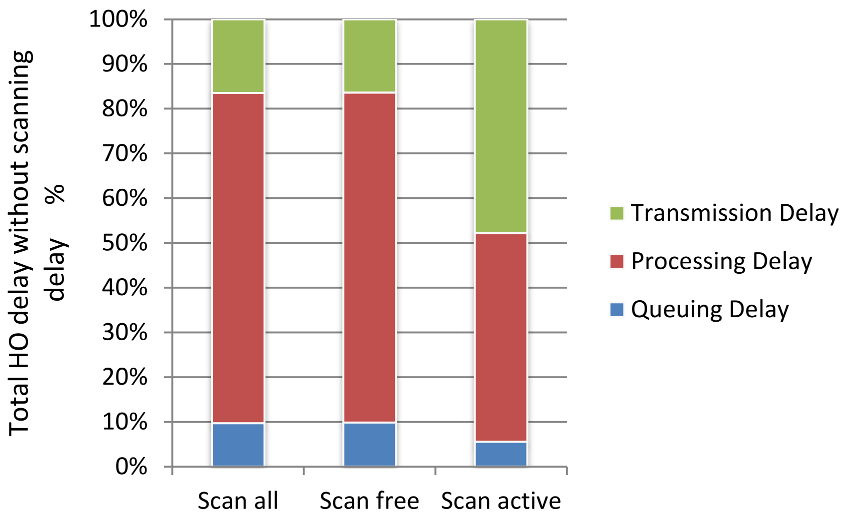

Figure 26. Percentages of total delay components

Queuing and transmission delays are related to the throughput; processing and transmission delays are related to the number of hops; and queuing delays are related to the request rate.

6.3.1 Throughput

In Figures 16 and 17 (Chapter 5), we saw that huge differences could be observed with 1 Mbps comparing with 11 Mbps when testing the Scan active scheme. After 11 Mbps, the delay values seem to be close. For the two other schemes, the changes through throughput values are unnoticed compared to Scan active. This is because the transmission delay, which accounts for 48% of the total delay of Scan active scheme, is dependent on throughput, while in the Scan all and Scan active schemes, this percentage (and its effect) drops to 16% of the total delay.

6.3.2 Number of MNs

As shown in Figure 18 in Chapter 5, the increasing number of MNs in the serving network will increase the delay of HO because the throughput decreases when the channel is shared by more than one MN. The effect occurs here is similar to the previous section ; Scan active is most affected when the throughput is decreased since 48% of its HO delay is transmission delay, which depends on throughput.

6.3.3 Number of hops on the IS-RLSS path

Both Scan all and Scan free are unaffected by the increased number of hops in IS-RLSS path because they do not make contact with RLSS after the HO is triggered. Scan active total delay increases dramatically with the increased number of hops, as shown on Figure 19 in Chapter 5. The transmission and processing delays consider the number of hops in their equations, which represent 94% of the total messaging delay (when scan delay is eliminated). Because of this, the total delay increases when the number of hops increases.

6.3.4 Number of request at RLSS

Increasing the number of requests received by RLSS only affects the queuing delay. The queuing delay represents 6% of the total delay of a single message in the Scan active scheme. Thus, the delay does not affect a lot by increase the number of requests on RLSS, as seen in Chapter 5, Figures 20 and 21.

6.3.5 MIH_Get_Info, Query_RLSS response messages size

Since the scanning delay of scanning one channel requires 0.1 sec, which is the 200% of the rest delay of HO process (MIH_Get_Info and Query_RLSS response/request messages with maximum size + L2 + L3), we can see that the effect of changing the message size on total HO delay is ineffective when the scanning time is increase due to increase number of active channels as shown in Figures 22 and 23 in previous chapter.

6.4 Comparing the improvement of all three schemes

The enhancements achieved by applying Scan free and Scan active schemes using the analytical model in the previous chapter are displayed in the following tables. Tables 13 and 14 show the percentages of the reduced total delay and its two components, scan and L3 HO (FMIPv6) delay. The L2 HO delay is not included since it does not show any improvement in all cases.

Table 13. Percentages of Total Delay Improvement of Scan Free and Scan Active Compared to Scan All

Enhance Scan all scheme by:	Scan free with 19 channels	Scan active
Total delay	36%	**From 94%, when scanning 1 channel, to 35%, when scanning 19 channels**
Scan delay	37%	**From 95%, when scanning 1 channel, to 37%, when scanning 19 channels**
FMIPv6 delay	0%	**38%**

Table14 Percentages of Total Delay Improvement of Scan Active Compared to Scan Free

Enhance Scan free scheme by:	Scan active
Total delay	**From 91% to 3% for scanning 1 to 18 channels and -2% for scanning 19 channels**
Scan delay	**From 92% to 3% for scanning 1 to 18 channels and -3% for scanning 19 channels**
FMIPv6 delay	**38%**

The information derived from the previous comparisons is as follows:

- We can see from the tables above that the reduction in the total delay is almost the same as that of the scanning delay, which confirms that the scanning delay causes most of the HO delay.
- The negative percentages -2% and -3%, shown in Table 14, indicate that the Scan active scheme will take longer than the Scan free scheme when the number of active channels equals the number of free channels. This additional delay is expected because of the extra four messages exchanged between MN and IS, and IS and RLSS.
- We see also that, even if we use MIH in the scan free scheme, the FMIPv6 delay is not reduced. This is because we assume in the Scan free scheme that the Free list obtained from IS contains only the number of free channels valid for two days and does not include any AP information. On the other hand, the Scan active scheme will contact IS when the HO is triggered and obtain Active list with up-to-date information. FMIPv6 can remove solicitation/advertisement messages by obtaining the requested information from IS, which decreases the L3 HO (FMIPv6) delay.

6.5 Tradeoff between Schemes

The main components of the total delay in all schemes are L2 HO, L3 HO, and IS query (pre-scanning phase) for Scan active only, which results in the following:

Scan all: FMIPv6 + Scan (m_1) + L2 → 7 messages + Scan (m_1) + 6 messages

Scan free: FMIPv6 + Scan (m_2) + L2 →7 messages + Scan(m_2) + 6 messages

Scan active: [FMIPv6 - (2 messages)] + [Scan(m_3)+4 messages] + L2 → 5 messages + Scan(m_3) +4 messages + 6 messages

Deleting FMIPv6 and L2, m=30 channels:

Scan all: Scan (30) = 3000 ms

Scan free: Scan (m_2) = m_2*100

Scan active: -2 messages+ Scan (m_3) + 4 messages =- 5.2 ms + m_3*100 + 28.7 ms

=m_3*100 + 23.5 ms

Thus, in the best case, with a high WiFi data rate (300 Mbps) and a minimal number of hops, the Scan active scheme has a delay of 23.5 ms more than other schemes, which is equivalent to time require to passively scanning 23.5% of one channel. When we change the throughput, the number of hops, and the request rate, separately, we get the values shown in Table 15.

Table 15. Scan Active Extra Delay with Equivalent Time of Scan Channels

Parameter	Value	Extra delay of Scan active	Equivalent scanning cost
Throughput	900 Kbps	514.1-2.6 = 511.5 ms + scan active channels delay	≈ scan 6 channels
	1 Mbps	485.8-14.9 = 470.9 ms + scan active channels delay	≈ scan 5 channels
Hops in RLSS path	10 nodes	103.8-5.2= 98.6 ms + scan active channels delay	≈scan 1 channel
	50 nodes	438-5.2= 432.8 ms + scan active channels delay	≈scan 5 channels
Queuing delay on RLSS	1000 requests	28.8-5.2= 23.6 ms + scan active channels delay	≈scan 1 channel
	27250 requests	32.2 -5.2 27 ms + scan active channels delay	≈scan 1 channel

Table 15 shows that number of hops gives us the extra cost equivalent to time required to scan 5 channels when assuming 50 hops. Moreover, we can conclude that with every ten additional hops, we lose the amount of time equal to scanning one channel. With 255 hops (maximum allowed value), the delay increases by 2144.8 ms, which is equivalent to scanning 22 channels. In this case, if the MN retrieves more than eight active channels, the Scan active scheme will be worse than the Scan all scheme since it requires more time than “scan all 30 channels” in Scan all. Queuing delay causes the shortest delay, since it takes a maximum of 27 ms. The delay caused by throughput is less than the delay caused by the number of hops.

6.6 WhiteFi to WiFi HO

The proposed schemes to improve the scanning phase in this thesis cannot be applied in the case of handing off to WiFi. The nature of the TV band is different since it is a licensed band and there are rules set regarding its use. WiFi operates on an ISM band, which is unlicensed. In the scanning phase, active scanning is allowed, which will reduce the time significantly, so scanning all channels does not lead to a bad result. To further reduce the scanning delay, IS gives the MN only the active channels with their related information. This is similar to our Scan active scheme, except that we cannot actively scan these channels in our scenario.

6.7 Conclusion

Scan active performs well until we change the network conditions. Fifty hops or more in the path of IS-RLSS will cost the equivalent amount of time to scanning five channels or more (assuming throughput is equal to or less than 1 Mbps). While Scan active can exceed Scan all with extreme changes in the conditions, Scan free consistently shows better results than Scan all, and in the worst case, when all 30 channels are free, it shows the same performance due to using the same messages. In

Scan active, a balance between the delay and the number of scanning channels should be considered.

Chapter 7

Conclusions and Future Work

7.1. Research Summary

In this thesis, we propose integration between IS in MIH and RLSS in WhiteFi architecture. We produce two techniques to reduce the scanning delay using IS via an MIH protocol. The first scheme, Scan free, depends on the MIH_Get_information request/response. In Scan free, IS now know about WhiteFi APs existing in the area by contact RLSS. If WhiteFi is available nearby, IS can retrieve a Free list, which is updated every 48 h. This list is included within each MIH_Get_Information response received by MN. The second technique is to send a special request to IS to retrieve the Active list from RLSS. When MN chooses to HO to WhiteFi, it has two choices, the first is to start passively scanning the channels from the Free list or to sending a request for Active list. MIH not only decreases the scanning phase delay, it also reduces the FMIPv6 delay by eliminating the first two messages of MD in Scan active scheme. To evaluate these mechanisms, we compared them with the base case, Scan all, in which all 30 channels are passively scanned with a 3 sec delay. The total HO delay, taken from the moment after the HO is triggered until the FMIPv6 message FNA is sent, is calculated using the analytical model. The total HO delay is equal to the summation of the scanning and its related messages, L2 HO, and L3 HO delays. The delay of each message in each previous component is equal to the summation of propagation, transmission, and queuing delays. The result shows that the proposed techniques perform better than the base case. Some parameters were changed to compare the behavior of the total delay.

7.2. Conclusion of Results and Findings

1. Scan active is the best scheme to adopt in typical conditions.
2. Changing conditions such as throughput will affect the performance of Scan active since it uses four additional messages to contact IS and RLSS.
3. Changing the throughput will increase the total delay of Scan active in rates less than 11 Mbps.
4. Since Scan active contacts RLSS, increasing the number of hops in the IS–RLSS path will increase the total delay and it may exceed the Scan all delay.
5. By increasing the RLSS queuing delay, delay increasing in micro and does not affect the total delay.
6. Scan free is better than Scan all, and in the worst case when all channels are free, it is equal to it. It is more stable against changing network conditions. Even with changing the condition, the increasing delay for both is equal since they have same messages. The only value of difference between them is the scan delay.

7.3. Recommendations

As a result of this work, Scan free drawback is the probability of wasting time scanning empty channels. Scan free doesn't cost MN any extra delay. Even with worst case when all Free list equal 30, Scan free is equal to Scan all. Scan active is consider to be the best scheme since it expected to scan less number of channels but with extra delay due to querying messages. This extra delay value is less than the delay of scan one channel with perfect environment and increased with network conditions change. Therefore, we recommended that, if MN chooses to use Scan active, depending on the number of retrieved channels and the delay of query process, the MN should decide either to scan all channels retrieved in Active list or choose only some of them. The algorithm and criteria to be used provides the direction of future work.

LIST OF REFERENCES

[1] J. Schiller, *Mobile Communications*: Addison Wesley, 2007.

[2] S. Rizvi, *et al.*, "An overview of vertical handoff decision policies for next generation wireless networks," in *Circuits and Systems (APCCAS), 2010 IEEE Asia Pacific Conference on*, 2010, pp. 88-91.

[3] N. Capela, *et al.*, "An Architecture for Optimized Inter-Technology Handovers: Experimental Study," in *Communications (ICC), 2011 IEEE International Conference on*, 2011, pp. 1-6.

[4] Y. Benkaouz, *et al.*, "Performance analysis of WiFi/WiMax vertical handover based on media independent handover," in *Multimedia Computing and Systems (ICMCS), 2012 International Conference on*, 2012, pp. 36-40.

[5] P. Machan, *et al.*, "Performance of mobility support mechanisms in a heterogeneous UMTS and IEEE 802.11 network offered under the IEEE 802.21 standard," in *Information Technology, 2008. IT 2008. 1st International Conference on*, 2008, pp. 1-4.

[6] S. Srikanteswara and D. Choudhury, "A review of TV Whitespace portable devices," in *Radio and Wireless Symposium (RWS), 2010 IEEE*, 2010, pp. 480-483.

[7] T. Baykas, *et al.*, "Overview of TV White Spaces: Current regulations, standards and coexistence between secondary users," in *Personal, Indoor and Mobile Radio Communications Workshops (PIMRC Workshops), 2010 IEEE 21st International Symposium on*, 2010, pp. 38-43.

[8] B. S. Ghahfarokhi and N. Movahhedinia, "A survey on applications of IEEE 802.21 Media Independent Handover framework in next generation wireless networks," *Computer Communications*, vol. 36, pp. 1101-1119, 2013.

[9] E. Insam, "Chapter 5 - LAN Access Technologies," in *TCP/IP Embedded Internet Applications*, E. Insam, Ed., ed Oxford: Newnes, 2003, pp. 109-143.

[10] M. F. Finneran, "Chapter 1 - The Convergence of Wireless LANs and VolP," in *Voice Over WLANS*, M. F. Finneran, Ed., ed Burlington: Newnes, 2008, pp. 1-26.

[11] M. F. Finneran, "Chapter 5 - 802. 11 Radio Link Specifications," in *Voice Over WLANS*, M. F. Finneran, Ed., ed Burlington: Newnes, 2008, pp. 103-133.

[12] M. F. Finneran, "Chapter 4 - Media Access Control Protocol," in *Voice Over WLANS*, M. F. Finneran, Ed., ed Burlington: Newnes, 2008, pp. 71-101.

[13] T. Baykas, *et al.*, "Developing a standard for TV white space coexistence: technical challenges and solution approaches," *Wireless Communications, IEEE,* vol. 19, pp. 10-22, 2012.

[14] C. Cordeiro, *et al.*, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, 2005, pp. 328-337.

[15] K. G. Shin, *et al.*, "Cognitive radios for dynamic spectrum access: from concept to reality," *Wireless Communications, IEEE,* vol. 17, pp. 64-74, 2010.

[16] C. Stevenson, *et al.*, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *Communications Magazine, IEEE,* vol. 47, pp. 130-138, 2009.

[17] "Capacity Considerations for Secondary Networks in TV White Space," *Mobile Computing, IEEE Transactions on,* vol. PP, pp. 1-1, 2014.

[18] L. Zhou, *et al.*, "Design and implementation of a Wi-Fi prototype system in TVWS based on IEEE 802.11 af," in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, 2013, pp. 750-755.

[19] A. B. Flores, *et al.*, "IEEE 802.11af: a standard for TV white space spectrum sharing," *Communications Magazine, IEEE,* vol. 51, pp. 92-100, 2013.

[20] D. Lekomtcev and R. Maršálek, "Comparison of 802.11 af and 802.22 standards–physical layer and cognitive functionality," *Elektro Revue,* vol. 3, pp. 12-18, 2012.

[21] K. Hyoil and K. G. Shin, "Understanding Wi-Fi 2.0: from the economical perspective of wireless service providers [Dynamic Spectrum Management]," *Wireless Communications, IEEE,* vol. 17, pp. 41-46, 2010.

[22] Y. Yanpeng, *et al.*, "On the capacity of Wi-Fi System in TV white space with aggregate interference constraint," in *Cognitive Radio Oriented Wireless Networks (CROWNCOM), 2013 8th International Conference on*, 2013, pp. 123-128.

[23] J. Márquez-Barja, *et al.*, "An overview of vertical handover techniques: Algorithms, protocols and tools," *Computer Communications,* vol. 34, pp. 985-997, 2011.

[24] A. A. Yussuf, *et al.*, "A review of VHD approaches in next generation wireless networks," in *Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on*, 2012, pp. 363-367.

[25] X. Yan, *et al.*, "A survey of vertical handover decision algorithms in Fourth Generation heterogeneous wireless networks," *Computer Networks*, vol. 54, pp. 1848-1863, 2010.

[26] J. Wozniak, "Mobility management solutions for IP networks," in *Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2012 XVth International*, 2012, pp. 1-11.

[27] K. N. Ashraf, *et al.*, "Survey and analysis of mobility management protocols for handover in wireless network," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, 2013, pp. 413-420.

[28] L. Jong-Hyouk, *et al.*, "Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols," *Industrial Electronics, IEEE Transactions on*, vol. 60, pp. 1077-1088, 2013.

[29] A. A. Bathich, *et al.*, "IEEE 802.21 based vertical handover in WiFi and WiMAX networks," in *Computers & Informatics (ISCI), 2012 IEEE Symposium on*, 2012, pp. 140-144.

[30] M. Q. Khan and S. H. Andresen, "An Intelligent Scan Mechanism for 802.11 Networks by Using Media Independent Information Server (MIIS)," in *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*, 2011, pp. 221-225.

[31] M. Q. Khan and S. H. Andresen, "Zero Scanning Time for 802.11 Networks by Using Media Independent Information Server (MIIS)," in *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on*, 2012, pp. 467-473.

[32] M. Q. Khan and S. H. Andresen, "The implications of zero scanning time on MIPv6 handover delays by using Media Independent Information Server (MIIS)," in *Communications (APCC), 2011 17th Asia-Pacific Conference on*, 2011, pp. 324-329.

[33] A. G. Niteshkumar, *et al.*, "An Advance Approach to Reduce Handover Delay by Reducing Scanning Delay Using Media Independent Handover in 802.11," in *Computing Sciences (ICCS), 2012 International Conference on*, 2012, pp. 159-162.

[34] A. Diab, *et al.*, "Analysis of proxy MIPv6 performance compared to fast MIPv6," in *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, 2008, pp. 579-580.

[35] V. Visoottiviseth and P. Ngamtura, "On the performance of MIPv6 and FMIPv6 based on real IPv6 applications over IEEE 802.11g testbeds," in *Communications and Information Technologies (ISCIT), 2010 International Symposium on*, 2010, pp. 1217-1222.

[36] M. Boutabia and H. Afifi, "MIH-based FMIPv6 optimization for fast-moving mobiles," in *Pervasive Computing and Applications, 2008. ICPCA 2008. Third International Conference on*, 2008, pp. 616-620.

[37] Y. Han, *et al.*, "A cross-layer UMTS/WLAN handover algorithm using optimized MIH," in *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on*, 2009, pp. 67-71.

[38] K. Moon, *et al.*, "Network-based seamless handover framework providing QoS in heterogeneous wireless networks," in *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*, 2009, pp. 254-258.

[39] M. Boutabia and H. Afifi, "Maximizing predictive mode probability in fast handovers for mobile IP," in *Telecommunications (ICT), 2013 20th International Conference on*, 2013, pp. 1-5.

[40] A. B. Forouzan, *Data Communications & Networking (sie)*: Tata McGraw-Hill Education, 2006.

[41] N. Mir, *Computer and communication networks*: Pearson Education, 2006.

[42] L. Shou-Chih, *et al.*, "Architecture for mobility and QoS support in all-IP wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 22, pp. 691-705, 2004.

التسليم بين شبكتي WiFi-WhiteFi : الإشارات و الآداء

بدور سعيد عبدالله باوزير

المستخلص

أصبحت الشبكات اللاسلكية اليوم أكثر أهمية نظرا للانتشار الواسع للهواتف الذكية. لتحقيق الاتصال الأفضل دائما ، الجهاز المحمول يجب أن يغير نقطة اتصاله متى ما دعت الحاجة للحفاظ على جودة الخدمة. التكامل بين الشبكات اللاسلكية يساعد الجهاز للانتقال فيما بينهم. التسليم هو عملية تغيير نقطة ارتباط الجهاز المحمول. IEEE 802.21هو بروتوكول لتوحيد هذه العملية بشكل مستقل بغض النظر عن نوع الشبكتين المعنيتين بعملية الانتقال. المساحة البيضاء لطيف ال TV هي الطيف الراديوي المرخص و غير المستخدم والتي توفر انتشار اعلى واختراق للأبنية بالمقارنة مع الأطياف الأخرى. المستخدمون الأساسيون لطيف الTV يحتلون القنوات لفترة معينة من الزمن، وهذا يعني توفر أطياف المساحات البيضاء في موقع معين يمكن أن تختلف مع مرور الوقت. منظمة ال FCC قامت بتحديد مجموعة من القنوات لاستخدامها من قبل المستخدمين الثانويين (غير المرخصين) عندما لا تستخدم هذه القنوات من قبل المستخدمين الأساسيين (المرخصين). "WhiteFi" IEEE 802.11af هي شبكة جديده وهي عبارة عن تعديل لطبقتي ال MAC / PHY للشبكة IEEE 802.11للسماح لها باستخدام المساحات البيضاء لطيف ال TV . الـ WhiteFi يمكن أن تستخدم لملء الفجوات بين شبكات WiFi بسبب تغطيتها الكبيرة. التسليم بين هذه الشبكتين تعطي المستخدمين خيارا منخفض التكلفة. يدرس هذا العمل التسليم بين شبكتي WiFi و WhiteFi. في شبكات ال IEEE 802.11 تأخذ عملية مسح القنوات حيز كبير من وقت التسليم الكلي. عملية المسح تتم بطريقة passive حيث ينتظر المستخدم 100 م ث لكل قناة في انتظار ال beacon التي ترسلها نقاط الاتصال أو بطريقة active حيث لاينتظر المستخدم بل يقوم هو بإرسال طلب اتصال على كل قناة و جمع الردود. عموما المسح بطريقة active يحتاج لوقت أقل وخصوصا عندما تكون القناة فارغة. في شبكة WhiteFi خصوصا هذا الوقت سوف يتزايد بسبب زيادة عدد قنوات طيف ال TV مقارنة مع شبكة WiFi التقليدية وعدم السماح للمستخدم باستخدام طريقة active في عملية المسح. باستخدام بروتوكول IEEE 802.21 هذا العمل يقترح طريقتين للتقليل من التأخير الناتج عن عملية المسح. أولا, "Scan Free" حيث يوجد لدى المستخدم جدول زمني للمساحات البيضاء لطيف TV المتوفرة في المنطقة من خلال الاستعلام من الخادم (IS) وهذه القائمة تحدث كل 48 ساعة. ثانيا، " Scan active" حيث يتم الاستعلام لاسترداد القنوات النشطة الحالية من الخادم المحلي RLSS مما يؤدي لفحص عدد أقل من القنوات الذي يؤدي بدوره إلى تقليل الزمن الكلي للتسليم. أداء هذين المقترحين تم تقييمها باستخدام نموذج تحليلي، ومقارنتهما بالطريقة التقليدية "Scan all" حيث يتم مسح كل القنوات. تظهر النتائج أن مسح القنوات النشطة فقط يقلل زمن المسح والخطر الناتج عن تغير ظروف الشبكة لن يؤثر على التأخير إذا كان عدد القنوات النشطة قليل. "Scan free" هو الأكثر استقرارا لكن مع خطر إضاعة الوقت في مسح القنوات الفارغة.

التسليم بين شبكتي WiFi-WhiteFi : الإشارات و الآداء

بدور سعيد عبدالله باوزير

بحث مقدم لنيل درجة الماجستير في علوم الحاسبات

د.غادة الدباغ
د.نادين عكاري

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبدالعزيز
جدة – المملكة العربة السعودية
فبراير 2015 م – ربيع ثاني 1436 هـ

بسم الله الرحمن الرحيم

قال تعالى ﴿ وَمَا تَوْفِيقِي إِلا بِاللهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ ﴾
سورة هود آية ٨٨

التسليم بين شبكتي WiFi-WhiteFi : الإشارات و الآداء

بدور سعيد عبدالله باوزير

بحث مقدم لنيل درجة الماجستير في علوم الحاسبات

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبدالعزيز
جدة – المملكة العربة السعودية
فبراير 2015 م – ربيع ثاني 1436 هـ