Developing a Policy Based Algorithm for mobile devices to Access Neighboring Wi-Fi APs in Enterprise Environment

Conducted By:

Riashad Noor - 12201116

Muhammad Mutasim Billah – 13101275

MD. Ashraful Alam - 16201101

Abu Nayeem MD. Mustakim - 17141026

Supervised By:

Dr. Amitabha Chakrabarty

Assistant Professor

Department of Computer Science and Engineering

BRAC University

Submission Date: 18th May 2017

Declaration

This is to certify that this final thesis report entitled **'*Developing a Policy Based Algorithm for mobile devices to Access Neighboring Wi-Fi APs in Enterprise Environment*'** is submitted by the authors for the purpose of obtaining the degree of Bachelor of Science in Computer Science, and the degree of Bachelor of Engineering in Computer Science and Engineering. We hereby declare that all the instances of work presented in this thesis are original and inspirations for the work that we have made use of have been duly accredited with proper referencing.

Signature of Supervisor

Dr. Amitabha Chakrabarty

Signature of Authors

MD. Ashraful Alam

Riashad Noor

Muhammad Mutasim Billah

Abu Nayeem MD. Mustakim

Acknowledgements

We are expressing our heartfelt gratitude to our supervisor, Dr. Amitabha Chakrabarty, Assistant Professor of the Department of Computer Science and Engineering of BRAC University, for laying the foundation for our thesis concept and providing his valuable ideas, insight and guidance at each and every step of the development process.

Additionally, we would like to thank Jinghao Shi, Liwen Gui, Dimitrios Koutsonikolas, Chunming Qiao and Geoffrey Challen of Dept. of Computer Science and Engineering, University at Buffalo for their work on Reciprocal Wi-Fi Sharing for home environment, which served as a starting point and major reference source for our thesis. We extend this appreciation towards authors from various other sources who have provided all the relevant information in their work that has made the completion of this thesis possible.

Furthermore, we would like to thank our family and friends for their continued support and encouragement throughout. Without them, this would not have been made possible, as they have helped push us further and further to reach our desired destination.

Last, but not least, we would like to thank our peers who have lent their support, advice and much appreciated words of encouragement. Their valuable input and suggestions with respect to our thesis is thoroughly appreciated.

Abstract

Wireless technology has been extensively used in every branch of life relating to internet usage. The AP acts as a central transmitter and receiver of wireless radio signals, which then usually connects to a hub, switch, or router via a wired network. Increasing the number of Wi-Fi access points provides network redundancy, better range, support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. It has become so simple that any compatible device can connect to the Internet via a WLAN network and a wireless access point (AP). For that, in enterprise environment Wi-Fi system gets the priority for accessing the Internet. Enterprise environment is necessarily dependent on multiple access points (APs) because there is significant number of users and wide area to be covered efficiently. Often, it happens that a wireless device connected to a particular Access Point (AP) and accessing internet with that network, gets signal from other APs of neighborhood. And it is observed that at some point some neighborhood AP's signal strength is stronger than the signal strength of the AP it is connected to, and the device can get better Internet performance from the neighbor APs than its own Home AP. For this situation, or situation like this, it can be technologically and economically beneficial use any of neighbor networks. So, we developed an algorithm of two parts and created an application with that algorithm to allow the user to use AP from neighborhood with better internet performance.

Index Terms — Wi-Fi, Access Point, AP, Signal Strength, Channel, Frequency, Bandwidth, Home, Neighbor, Algorithm, Access, Android Smart Phone, Control, Security, Better Network, Switching, Buffer.

Table of Contents

Chapter 1

Introduction

For a long period of time, it was not possible to have open communications systems on the physical level in networking. Before Wi-Fi system, in a world of wires, the meaning of network access was physical access. Wi-Fi system as wireless networking enabled the technical possibility of a completely open network [7]. And smart-phone has introduced us with a new scope that users or consumers can use the Wi-Fi network to make calls or browse the internet without paying for cellular network. So, undoubtedly this is the new reality for using internet. People now mostly use the Wi-Fi system to access the internet and they use smart-phones or android based devices as equally they use computer, laptop [9]. People now use Wi-Fi for personal usage in home environment, and for commercial usage in enterprise environment. In enterprise environment Wi-Fi system is used to meet the commercial purposes, and generally a larger Wi-Fi range has to be covered. So, in enterprise environment they use multiple access points (APs) with distinct ranges. And multiple Wi-Fi access points (APs) provide network redundancy, better range, and support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. Each access point works for a certain range to cover and has certain group of users to access. For most cases, each access point can have a particular or common SSID and their network performance varies at any given point of time. Another concern is the using of smart-phone or android based devices or other lighter mobile devices are increasing rapidly. There is no obstacle to move with a smart-phone, so the dependency on smart-phone to access internet is also increasing. It is very natural that, in an enterprise or commercial space, someone of that place has to move or go to different parts of that space. And when he/or she does that, he may need to access the internet and he/she may not get the better internet performance from his/her own access point (AP). It is true for every person of that place. So an attainable sharing system of APs will help in a sustainable way in an enterprise environment [1].

1.1 Motivation

Our goal is more than sharing the Wi-Fi APs. Our goal is one step forward in the wider approach of how we access the internet. In Wi-Fi network system, any license is not required to use the Wi-Fi spectrum and we are trying to make the beneficial uses of this unlicensed open spectrum [7]. And we think the uses of unlicensed spectrum can lead us to better functioning of routers, smart-phones, android based devices, laptops and with some conditions, of computers also. For enterprise environment, uses of unlicensed spectrum have led us to think about more productive technology or system. In enterprise environment, sharing the Wi-Fi APs through using the unlicensed spectrum will provide the faster and better connectivity [1]. We thought that if we could make a system that will make the uses of internet cost effective and technologically effective. Our main focus was to create an algorithm that would be definitely economically and technologically beneficial [2]. We also thought of that any kind of deployment of our algorithm will ensure the security of control of access points (APs) [3].

Chapter 2

Background of Study

Our algorithm of sharing Wi-Fi access points (APs) works for many problems of the real scenario, and provides the most efficient attainable solution at any given point of time, but there is a different set of problems and environment that need to be addressed and worked out on for unquestionable success. So, we tried to find out the problems and lacking the available algorithm and systems do have, that is a point of interest for our policy based algorithm to access the neighboring APs in enterprise environment. We tried to minimize and deal with as much issues concerning the Wi-Fi network system and APs in enterprise environment as possible.

2.1 Wi-Fi and Multiple APs.

In Wi-Fi network system, the AP works as a central transmitter and receiver of wireless radio signals, that AP usually connects to a hub, switch, or router via a wired network. Different kinds of APs with differing radios, antennas, and performance rates do the work [5].

Now, in office or enterprise environments, Wi-Fi network system and multiple access points are used serve their purposes, such as:

- **Office with larger area and multiple floors:** Secure Wi-Fi system improves productivity, reduces switch port and cabling costs, and keeps online available to office inexpensively. And as they have a large area and large number of user to cover, they use multiple APs.
- **Campus of School, College and University:** Wi-Fi system and a large number of access points (APs) are used to ensure the internet access for student, teacher and stuffs.
- **Healthcare and Hospital:** Wi-Fi speeds up delivery of medical images. All the patient records and information about appointments for doctors are stored in internet and those information changes so dynamically. So, to keep the larger area functioning and to keep

the large number of doctors, nurses and stuffs connected to the internet, hospitals and healthcare institution uses multiple APs.

- **Small office, shop, food court and super shop:** Small office doesn't need a large number of APs, but they use multiple APs to provide the internet access to their workers and guests. Many restaurants, food courts, shops and super shops provide free Wi-Fi service to their customers, and their stuffs need the internet access also, so they use multiple access points (APs).
- **Manufacturing place and Factory:** Internet is essential for any factory and manufacturing place to function. Wi-Fi system and multiple APs are necessary for that kind of place because of large area with enough number of users.

There are many other enterprise-based and commercial uses of Wi-Fi multi-access point implementations in organizations that range from several to thousands of users making wireless connectivity an essential element to building an enterprise network.

2.2 Wi-Fi and Smart-Phone

These were merely the technical details of Wi-Fi configuration and its various peripherals. As of recent times, Wi-Fi has been a relatively new and exciting feature to the common man. The world of smart-phones has brought on new possibilities where cables have become a redundancy over time. The efficiency of a common smart-phone has replaced most of our daily appliances to become an integral part of our lives where we can share the most exciting moments of our lives with a single touch on a screen or the push of a button. The future of Internet usage on smart-phones is bright and when combined with the numerous hotspots that are taking over the world, it keeps getting more exciting [9].

There are four ways to use WPS to add a device to a network — the push-button method, the PIN method, the NFC method and the USB method. NFC and USB are optional ways to set things up, so the user's Wi-Fi certified device may not support one or both. Android devices typically use the Push Button or PIN method, but in theory could support NFC and USB as well.

To use WPS, the users' need it enabled on the router they want to connect to. Most Android users will then push a button on their router, then choose WPS Push Button from the menu if the Wi-Fi settings. Alternatively, a device can connect to the router's control panel interface and use the PIN method. Do note that using a WPS PIN makes the network vulnerable to a very specific and very difficult to perform brute-force attack. Hence, disabling PIN access to Wi-Fi is recommended.

2.3 Literature Review

To observe how our proposed algorithm and sharing the network create additional value in how we approach the Wi-Fi APs and access the internet. Think of two persons, A and B. They both work in the same office, but their work stations are in different part of their office [2]. Their APs or routers are different, and those cover a certain range. A and B often move to the other parts of the office for some official purposes, and occasionally they go to each other's work station to meet the mutual purposes. Consider the world as it is today: they can use their access points (APs), but they can't use each other's APs. Here is the key point – at many point of that office, A gets better signal strength from any other AP, but very weak signal strength from his AP. And it is true for B as well as for other stuffs of that office. That means the range of different APs overlap with the range of other APs. And at any given place of that office and at any given point of time, a user designated to a certain AP can have not only the better signal strength, but the potential of better internet performance by any other AP. In this circumstance, it would be definitely beneficial for that user to get internet access via that AP with the potential [6]. But he is not allowed to get connectivity from the AP other than the AP he is designated to. We developed an algorithm and a system that will make him access the internet via the AP with more potential without his knowing about the password and other things.

The main points about the algorithm we developed are:

1. Our algorithm works in a way that it can change its AP (Access Point) and that AP can allow the device to access the internet.

2. For using neighboring AP, the things should be considered are signal strength, bandwidth, and channel.

3. We created an Android-based application that helps the device to switch its AP.

4. Our algorithm has actually two portions. For both portions of our algorithm, working as one body makes them practically attainable.

5. The Two portions are: a) Achieve the access Algorithm and b) Establish the connection Algorithm.

6. Achieving the access Algorithm works for control and security.

7. Establish the Connection Algorithm makes decision when and which AP is better to be connected with.

8. Lastly, the device connects with the better one (AP)

Chapter 3

Wi-Fi in Physical Layer

Wireless technology has been extensively used in every branch of life relating to internet usage. Wi-Fi essentially uses radio waves to to transmit information across a network with devices based on the IEEE 802.11 standards. It is the widest used form of wireless connectivity medium used in the modern age. Wi-Fi is a trademark of the Wi-Fi Alliance. Hence, the term Wi-Fi-certified is used for products that are certified on completion of an interoperability testing. Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point.

An access point or hotspot has a range of about 20 meters indoors and greater range outdoors. Wi-Fi provides wireless connectivity to your devices by emitting frequencies between 2.4GHz - 5GHz, based on the amount of data on the network [15]. What makes Wi-Fi so powerful is its compatibility to almost every systems or devices, leading to the wide usage of wireless networks in schools, libraries, airports, hotels etc.

3.1 How does Wi-Fi work?

Wi-Fi technology may be used to provide internet access to devices that are within the range of a wireless network that is connected to the Internet. The coverage of one or more hotspots with overlapping coverage can extend from an area as small as a few rooms to as large as many square kilometers. Routers that incorporate a digital subscriber line modem or a modem and a Wi-Fi access point, often set up in homes and other buildings, provide Internet access and internetworking to all devices connected to them, wirelessly or via cable. Similarly, battery-powered routers may include a cellular Internet modem and Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks using the tethering technique.

Many modern smart-phones have a built-in Wi-Fi feature. For example, Android, Blackberry, Bada, IOS, Windows Phone and Symbian all use the feature. They can also incorporate the network usage as such so to even transmit as a hotspot. Modern laptops also have similar built-in features .

3.2 IEEE 802.11 standard

The IEEE 802.11 is a standard set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer connection in the 2.4, 3.6, 5 and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. In the market place, each revision tends to become its own standard [15].

3.2.1 Frequencies

A wireless network will transmit at a frequency level of 2.4 GHz or 5GHz to adapt to the amount of data that is being sent by the user. The 802.11 networking standards will somewhat vary depending mostly on the user's needs.

The 802.11a will transmit data at a frequency level of 5GHz. The Orthogonal Frequency-Division Multiplexing (OFDM) used enhances reception by dividing the radio signals into smaller signals before reaching the router. You can transmit a maximum of 54 megabits of data per second.

The 802.11b will transmit data at a frequency level of 2.4GHz, which is a relatively slow speed. You can transmit a maximum of 11 megabits of data per second.

The 802.11g will transmit data at 2.4GHz but can transmit a maximum of 54 megabits of data per second as it also uses an OFDM coding.

The more advanced 802.11n can transmit a maximum of 140 megabits of data per second and uses a frequency level of 5GHz [15].

3.3 Wi-Fi Radio Spectrum

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices.

Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels (12, 13) beyond the 11 permitted in the United States for the 2.4 GHz band, while Japan has three more (12–14). In the US and other countries, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the only non-overlapping channels is, therefore, not accurate. Channels 1, 6, and 11 are the only group of three non-overlapping channels in North America and the United Kingdom. In Europe and Japan using Channels 1, 5, 9, and 13 for 802.11g and 802.11n is recommended

802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap [15].

3.4 Devices

A **wireless access point (WAP)** connects a group of wireless devices to an adjacent wired LAN. An access point resembles a network hub, relaying data between connected wireless devices in addition to a (usually) single connected wired device, most often an Ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC Card. As of 2010.

Wireless routers integrate a Wireless Access Point, Ethernet switch, and internal router firmware application that provides IP routing, NAT, and DNS forwarding through an integrated WAN-interface. A wireless router allows wired and wireless Ethernet LAN devices to connect to a (usually) single WAN device such as a cable modem or a DSL modem. A wireless router allows all three devices, mainly the access point and router, to be configured through one central utility. This utility is usually an integrated web server that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a computer, as is the case with as Apple's AirPort, which is managed with the AirPort Utility on Mac OS X and iOS.

3.5 WPS

Wi-Fi Protected Setup (WPS; originally, Wi-Fi Simple Configuration) is a network security standard to create a secure wireless home network. Created by the Wi-Fi Alliance and introduced in 2006, the goal of the protocol is to allow home users who know little of wireless security and may be intimidated by the available security options to set up Wi-Fi Protected Access, as well as making it easy to add new devices to an existing network without entering long passphrases. Prior to the standard, several competing solutions were developed by different vendors to address the same need [15].

Chapter 4

Device and Wi-Fi Aps

In Wi-Fi system, there are two types of devices: Access Point (AP), and Client devices, here we will call it only ‘Device’. In simple terms, "router" would be the AP, and the client system is the Device. Devices can know an AP exists and is in range because the AP keeps broadcasting "beacons" -- by default it is 10 beacons per second. Within the beacon there's an informational element listing the SSIDs the AP handles, which is optional. When the broadcasting of beacons stop, Devices know the AP is dead or it is moved out of range.

To understand the way a Device gets connectivity and how well it gets we should know four facts.

a) The farther away from the router the device is, the worse the signal strength will be. Wi-Fi performance decreases.

b) The more wireless networks there are around, the worse Wi-Fi performance will be. It is because of conflicting transmission and channel overlapping.
c) When appliances such as cordless phones, microwaves, and security camera are on, Wi-Fi performance decreases because they create interference to Wi-Fi frequency.
d) When there are many users in an access point (AP), it affects the internet speed. If someone is doing something that hogging bandwidth, the Wi-Fi performance decreases.

So from above we can understand that there are some variables those can determine Wi-Fi performance. Among them, the major three are directly related to each particular AP or particular Network. They are Signal Strength, Channel Frequency and Bandwidth.

4.1 Signal strength in Wi-Fi

Wi-Fi signal strength is precarious. The most exact approach to express it is with dBm, which remains for decibels in respect to a mili watt. RSSI (Received Signal Strength Indicator) is a typical estimation also, yet most Wi-Fi connectors handle it in an unexpected way, so it's basic for applications to change over it to dBm. The main thing to comprehend about dBm is that we're working in negatives. - 30 is a higher signal than - 80, on the grounds that - 80 is a much lower number. Next, it's critical to realize that dBm does not scale in a direct manner like you'd expect, rather being logarithmic. That implies that signal strength changes aren't smooth and continuous [9].

3 dB off loss	-3 dB	Halves signal strength
3 dB of gain	+3 dB	Doubles signal strength
10 dB of gain	+10 dB	10 times more signal strength
10 dB of loss	-10 dB	10 times less signal strength

Table 4.1: The Rule of 3's and 10's highlights the logarithmic nature of dBm.

Signal Strength	**Quality**	**Review**	**Required For**
-30 dBm	Amazing	Strongest signal strength. The client can achieve this only be a few feet from the AP.	N/A

-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWi-Fi, streaming video
-70 dBm	Average	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Noise ratio is higher. User won't be able use due to poor signal strength	N/A

Table 4.2: How the quality varies with the signal strength

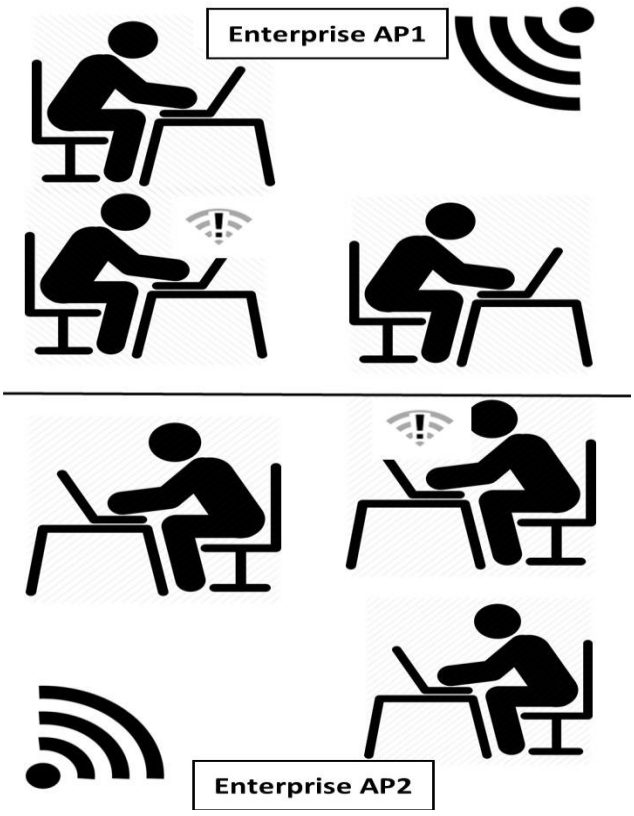


Figure 4.1.1: How the signal strength varies with distance in work place.

The image above shows the router connected to the devices in an enterprise floor. The laptop directly above has full signal strength, as generally the signal can penetrate through ceilings without any problems [9]. The laptop in the loft conversion is much further away; this weakens the signal slightly and some performance issues may be experienced.

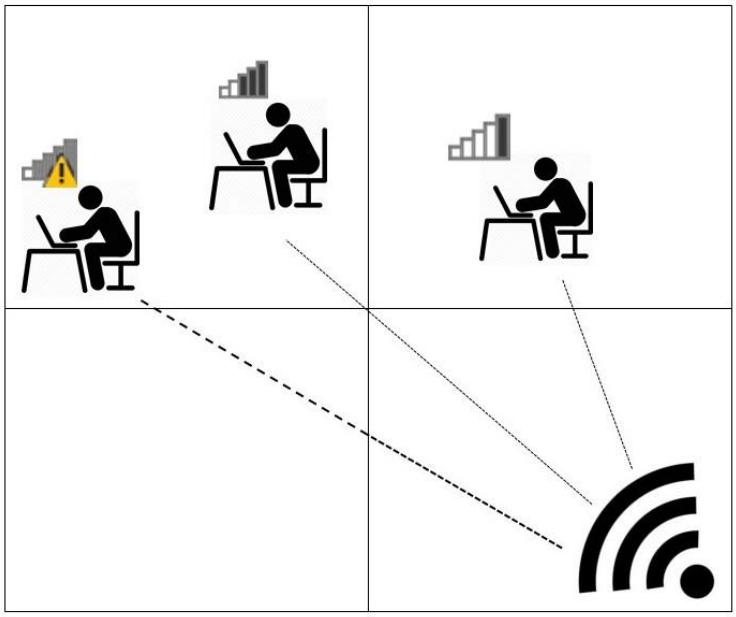


Figure 4.1.2: Distance affects the connectivity in same work place

As in the first example, the load bearing wall is also affecting the signal in other places. Line-of-sight is important for radio waves, as they only travel in straight lines. As the image shows, when the signal passes through the thicker wall the signal is degraded. Moving the laptop to another part of the office, where the signal just passes through thin walls, improves the signal.

4.2 Channels in Wi-Fi

All Wi-Fi enabled devices including user's gadgets and broadband switches convey over particular remote channels. Like stations on a customary TV, every Wi-Fi channel is assigned by a number that speaks to a particular radio correspondence recurrence. Wi-Fi gadgets consequently set and conform their remote channel numbers as a major aspect of the correspondence convention. OS and other tools on PCs and switches monitor Wi-Fi channel settings being utilized at any given time. Under typical conditions, clients don't have to stress over these settings. Be that as it may, clients and overseers may wish to change their Wi-Fi direct numbers in specific circumstances [10].

4.2.1 Basic segmentation of channels

Enhancing signal strength is unlike to adding more lights to get a brighter lounge room. Devices that transmit effectively, for example, routers, AP, and mobile phone base stations, can meddle with each other. To keep that, put them as far separated as could be allowed, and guarantee that they utilize diverse channels.

Devices that are made up with 802.11b and 802.11g can be tuned to one of 11 diverts in North America, 13 directs in Europe. In the event that encounter obstruction from overlapping wireless networks, each system ought to utilize one of the non-covering channels. These are channels 1, 6 and 11 in USA. Channels 1, 7 and 13 in Europe. This permits three systems to utilize a similar space with least impedance. On the off chance that you can not do that, pick channels as generally divided as could be expected under the circumstances, ideally no less than five channels separated. For instance, utilize channels 1 and 6, or channels 4 and 10.

Lamentably, you can't totally stay away from obstruction just by utilizing different channels. Wireless conventions 802.11b and 11g just have three non-covering channels. Whenever at least four directs are utilized as a part of a similar territory, the level of obstruction can increment prominently. On the off chance that you and your nearby neighbor both have a switch and a remote get to point, a sum of four effective transmitters are in nearness and you both experience some impedance.

In case you're encountering an extreme issue, a functional and friendly thing is to converse with your neighbors utilizing wireless systems that can be seen when you filter. Together, you can pick ideal channels for your individual systems. Tune your device to channels that no less than five channels separated. Along these lines, for instance, you may utilize channels 1 and 8, and your neighbor may utilize 5 and 11. Setting Energy to Half or quarter ought to be considered.

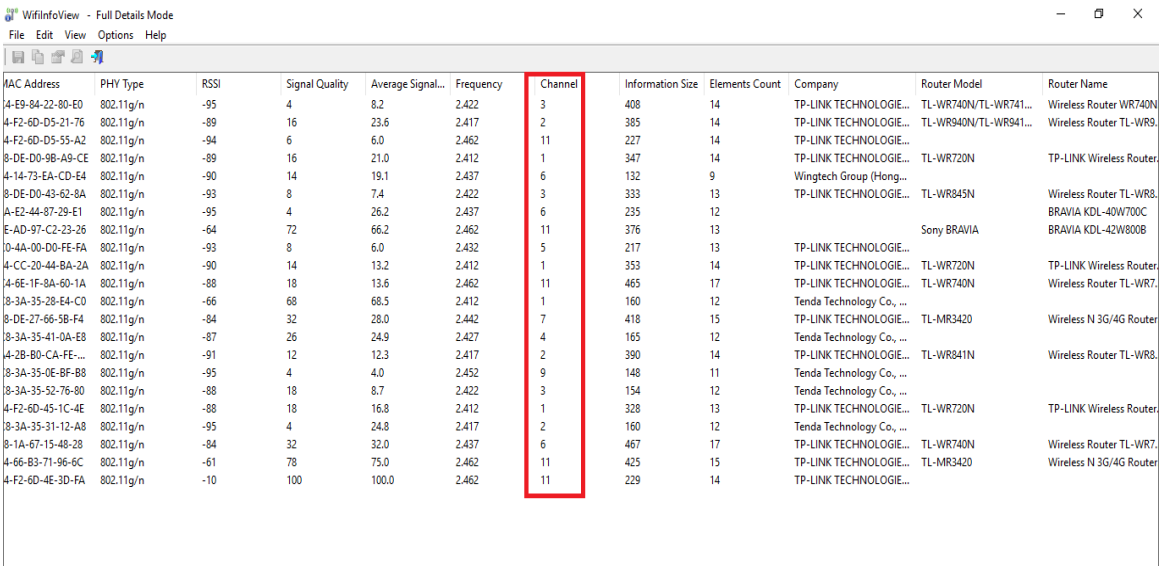
You may have the capacity to place routers and APs more distant far from each other inside your homes. All things considered, the sorts of physical hindrances that decrease your transmission run additionally diminish the signal that your neighbor wouldn't like to see.

4.2.2 2.4 GHz Wi-Fi Channel

Wi-Fi hardware in the U.S. and North America highlights 11 channels on the 2.4 GHz band:

- channel 1 works at an inside recurrence of 2.412 GHz
- channel 11 works at 2.462 GHz
- Rest of the channels work at frequencies in the middle of, uniformly dispersed at 5 MHz (0.005 GHz) interims.
- Wi-Fi adapt in Europe and different parts of the world additionally bolsters channels 12 and 13 running at the following higher recurrence levels 2.467 and 2.472, separately.

A couple of extra limitations apply in specific nations. For instance, 2.4 GHz Wi-Fi in fact bolsters 14 channels, despite the fact that channel 14 is accessible for old 802.11b hardware in Japan. Since each 2.4 GHz Wi-Fi channel requires a signal band about 22 MHz wide, radio frequencies of neighboring channels numbers essentially cover each other.



MAC Address	PHY Type	RSSI	Signal Quality	Average Signal...	Frequency	Channel	Information Size	Elements Count	Company	Router Model	Router Name
4-E9-84-22-80-E0	802.11g/n	-95	4	8.2	2.422	3	408	14	TP-LINK TECHNOLOGIE...	TL-WR740N/TL-WR741...	Wireless Router WR740N
4-F2-6D-D5-21-76	802.11g/n	-89	16	23.6	2.417	2	385	14	TP-LINK TECHNOLOGIE...	TL-WR940N/TL-WR941...	Wireless Router TL-WR9.
4-F2-6D-D5-55-A2	802.11g/n	-94	6	6.0	2.462	11	227	14	TP-LINK TECHNOLOGIE...		
8-DE-D0-9B-A9-CE	802.11g/n	-89	16	21.0	2.412	1	347	14	TP-LINK TECHNOLOGIE...	TL-WR720N	TP-LINK Wireless Router.
4-14-73-EA-CD-E4	802.11g/n	-90	14	19.1	2.437	6	132	9	Wingtech Group (Hong...		
8-DE-D0-43-62-8A	802.11g/n	-93	8	7.4	2.422	3	333	13	TP-LINK TECHNOLOGIE...	TL-WR845N	Wireless Router TL-WR8.
A-E2-44-87-29-E1	802.11g/n	-95	4	26.2	2.437	6	235	12			BRAVIA KDL-40W700C
E-AD-97-C2-23-26	802.11g/n	-64	72	66.2	2.462	11	376	13		Sony BRAVIA	BRAVIA KDL-42W800B
0-4A-00-D0-FE-FA	802.11g/n	-93	8	6.0	2.432	5	217	13	TP-LINK TECHNOLOGIE...		
4-CC-20-44-BA-2A	802.11g/n	-90	14	13.2	2.412	1	353	14	TP-LINK TECHNOLOGIE...	TL-WR720N	TP-LINK Wireless Router.
4-6E-1F-8A-60-1A	802.11g/n	-88	18	13.6	2.462	11	465	17	TP-LINK TECHNOLOGIE...	TL-WR740N	Wireless Router TL-WR7.
8-3A-35-28-E4-C0	802.11g/n	-66	68	68.5	2.412	1	160	12	Tenda Technology Co., ...		
8-DE-27-66-5B-F4	802.11g/n	-84	32	28.0	2.442	7	418	15	TP-LINK TECHNOLOGIE...	TL-MR3420	Wireless N 3G/4G Router
8-3A-35-41-0A-E8	802.11g/n	-87	26	24.9	2.427	4	165	12	Tenda Technology Co., ...		
4-2B-B0-CA-FE-...	802.11g/n	-91	12	12.3	2.417	2	390	14	TP-LINK TECHNOLOGIE...	TL-WR841N	Wireless Router TL-WR8.
8-3A-35-0E-BF-B8	802.11g/n	-95	4	4.0	2.452	9	148	11	Tenda Technology Co., ...		
8-3A-35-52-76-80	802.11g/n	-88	18	8.7	2.422	3	154	12	Tenda Technology Co., ...		
4-F2-6D-45-1C-4E	802.11g/n	-88	18	16.8	2.412	1	328	13	TP-LINK TECHNOLOGIE...	TL-WR720N	TP-LINK Wireless Router.
8-3A-35-31-12-A8	802.11g/n	-95	4	24.8	2.417	2	160	12	Tenda Technology Co., ...		
8-1A-67-15-48-28	802.11g/n	-84	32	32.0	2.437	6	467	17	TP-LINK TECHNOLOGIE...	TL-WR740N	Wireless Router TL-WR7.
4-66-B3-71-96-6C	802.11g/n	-61	78	75.0	2.462	11	425	15	TP-LINK TECHNOLOGIE...	TL-MR3420	Wireless N 3G/4G Router
4-F2-6D-4E-3D-FA	802.11g/n	-10	100	100.0	2.462	11	229	14	TP-LINK TECHNOLOGIE...		

Figure 4.2.1: Different channels for different networks and devices

4.2.3 5 GHz Wi-Fi Channel

5 GHz offers altogether a larger number of channels than does 2.4 GHz Wi-Fi. To evade issues with covering frequencies, 5 GHz gadget confines accessible channels to specific numbers inside a bigger range. This is like how AM/FM radio stations inside a neighborhood some partition between each other on the groups.

For instance, mainstream 5 GHz remote diverts in numerous nations incorporate 36, 40, 44, and 48 while different numbers in the middle of are not bolstered. Channel 36 works at 5.180 GHz with each channel balance by 5 MHz, so that Channel 40 works at 5.200 GHz (20 MHz balance), et cetera. The most elevated recurrence channel (165) works on 5.825 GHz. Hardware in Japan underpins an altogether unique arrangement of Wi-Fi channels that keep running at lower frequencies (4.915 to 5.055 GHz) than whatever remains of the world.

4.2.4 Why to Change Wi-Fi Channel

Many home systems in the U.S. use switches that as a matter of course keep running on channel 6 on the 2.4 GHz band. Neighboring Wi-Fi home systems that keep running over a similar channel create radio impedance that can bring about noteworthy system execution log jams for clients. Reconfiguring a system to keep running on an alternate remote channel limits these stoppages. Some Wi-Fi outfit, especially more seasoned gadgets, may not bolster programmed channel exchanging. Those gadgets will not be able associate with the system unless their default channel coordinates the neighborhood system's arrangement.

To change channels on a home remote switch, sign into the switch's design screens and search for a setting called "Channel" or "Remote Channel." Most switch screens give a drop-down rundown of bolstered channel numbers to browse.

Different gadgets on a nearby system will auto-distinguish and modify their channel numbers to match that of the switch or remote get to point with no activity required. In any case, if certain gadgets neglect to interface subsequent to changing the switch's channel, visit the product arrangement utility for each of those gadgets and roll out coordinating channel number improvements there. A similar design screens can likewise be checked at any future time to confirm the numbers being used.

4.2.5 Wi-Fi decides a particular channel

The decision of selecting channels can bigly affect bandwidth performance. You will likely pick settings that maintain a strategic distance from impedance from other systems administration and radio frequency devices [8]. This is particularly essential if your hardware utilizes the 802.11n or 802.11ac wireless systems administration standard. Consider conforming the divert choices in the accompanying circumstances:

- Sharing access through the neighborhood Wi-Fi APs.
- Enhancing the wireless coverage.
- Utilizing numerous wireless switches, which requires to utilize distinctive channels on the devices.

4.2.6 Picking the Best Wi-Fi Channel

In numerous conditions, Wi-Fi associations perform similarly well on any channel: At times the best decision is to leave the system set to defaults with no progressions [8]. Execution and unwavering quality of associations can fluctuate extraordinarily crosswise over channels, in any case, contingent upon the wellsprings of radio obstruction and their frequencies. No single channel number is intrinsically "best" in respect to the others.

For instance, a few clients like to set their 2.4 GHz systems to utilize the most minimal conceivable or most noteworthy conceivable channels (11 or 13, contingent upon nation) to maintain a strategic distance from mid-go frequencies since some home Wi-Fi switches default to the center channel 6. Be that as it may, if neighboring systems all do a similar thing, genuine obstruction and availability issues can come about. In outrageous cases, clients may need to facilitate with their neighbors on the channels each will use to keep away from shared impedance.

4.2 Bandwidth

In terms of computer networks, transmission capacity is utilized as an equivalent word for data transfer rate, the measure of information that can be conveyed starting with one point then onto the next in a given day and age (within a moment). Arrange data transmission is normally communicated in bits per second (bps); present day organizes regularly have speeds measured in

large number of bits per second (megabits every second, or Mbps) or billions of bits for every second (gigabits every second, or Gbps).

Take note of that data transfer capacity is by all account not the only component that influences data transfer speed: There is likewise packet loss, latency and jitter, all of which debase organize throughput and make a connection perform like one with lower transmission capacity. A system way for the most part comprises of a progression of connections, each with its own particular data transmission, so the end-to-end transfer speed is restricted to the data as most system admin can validate, organize data transmission is one of the more imperative calculates the outline and support of a useful LAN or WAN. Not at all like a server, which can be arranged and reconfigured for the duration of the life of the system, transfer speed is one of those components of system plan that is typically advanced best by designing the system effectively from the beginning [10].

Transfer speed alludes to the information rate that is bolstered by the system association or the interfaces that associate with the system. It is generally communicated regarding bytes per second (bps). Organize transfer speed speaks to the limit of the system administration, however it's critical to comprehend the refinement between hypothetical throughput and genuine outcomes. For instance, a 1000BASE-T (which utilizes unshielded curved match links) Gigabit Ethernet (GbE) system can hypothetically bolster 1,000 megabits for every second (Mbit/s), yet this level can never truly be accomplished by and by as a result of equipment and frameworks programming overhead. It is this very point makes computing transmission capacity a test of the least speed interface.

4.3.1 Deciding Access Point Bandwidth

It is a typical measuring error to utilize the hypothetical most extreme to gauge how much bandwidth an AP can really bolster, for instance, the hypothetical bandwidth for an AP with a 2x2 double band radio that can bolster up to 300Mbps for each radio would be 600 Mbps (300Mbps x 2). Expecting there are 25 simultaneous Wi-Fi clients in the territory, you could erroneously figure that each get to point can bolster 24Mbps for every client (600Mbps/25 clients).

Practically speaking, there are a few elements that will altogether lessen AP bandwidth versus realistic scenario:

- Protocol and bundle overhead - can diminish throughput by 40 to 50 %

- Slow or "far away" customers - customers that are further away or in a zone of weaker signal quality must stride down the transmission physical rate (PHY) rate to send the packet (e.g. a customer sending a packet at 1 Mbps will take 100 times longer than a customer sending a similar bundle at a PHY rate of 100Mbps), conceivably bringing on an extra half depreciation of throughput.

- Uneven distribution of customers - in a double band simultaneous AP, both groups can all the while bolster customer activity. Nonetheless, not all customers are double band and there is no certification that even the double band customers will equally disperse themselves in the vicinity of 2.4 and 5GHz. Arrange viability might be decreased by another half because of the conduct of the customers.

- Control activity – control movement traded between the AP and different customers at low PHY rates can additionally diminish accessible data transfer capacity by 25%.

- Other – co-channel and nearby channel obstruction, organize re-transmissions, and terrible conduct customers will additionally decrease AP throughput.

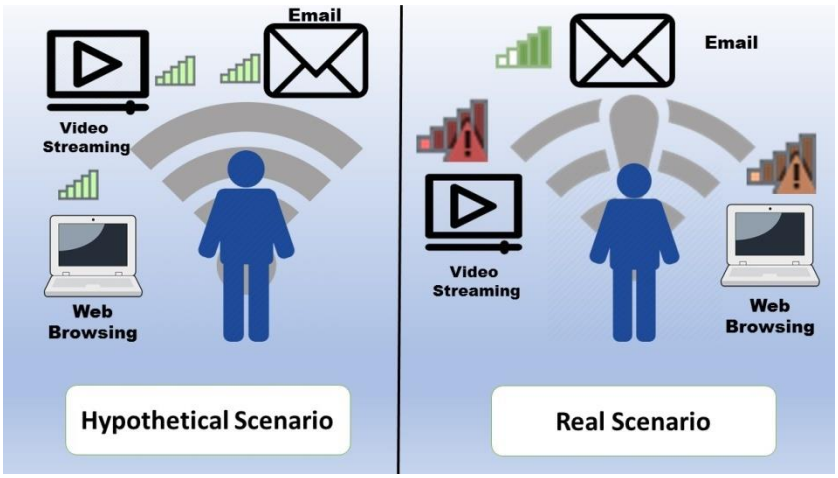


Figure 4.3.1: Bandwidth affects the internet performance differently

4.3.2 Setting up bandwidth requirements

When outlining high density wireless systems, it is basic to comprehend which applications will be utilized and how much transmission capacity. Every application will expend as far as throughput per client. First, we have to estimate how much bandwidth is required for basic applications, for example, web, sound, video, printing, document sharing, and web based testing. Increasingly and more schools are utilizing on the web video applications, for example, knowmia.com and youtube.com as an everyday instructing apparatus. As should be obvious from the outline, bandwidth necessities can differ from 2 to 4Mpbs for every client relying upon the video determination. Once the data transfer capacity per application is known, this number can be utilized to figure the data transfer capacity required per client. Notwithstanding the kind of uses to be utilized, data transfer capacity necessities will change in light of the quantity of expected clients on the wireless system. As more clients get to the system bandwidth per client goes down bringing on slower transmission rates. In the event that the system comprises of blended customers (11a, b, g and 11n modes), the normal throughput per customer will likewise go down with the more prominent the quantity of legacy customers [10].

Once the sorts of uses are recognized and the transmission capacity per kind of use is resolved, you can build up the total data transfer capacity required by increasing the aggregate Mbps by the quantity of expected clients in the scope range.

4.4 *Switching: A solution?*

Despite being one of the quintessential elements in enterprise network spaces, the limitations of Wi-Fi do remain. It is extremely difficult to maintain a proper connection on the move, especially when the current access point is far away or when there is a load-balancing issue on the routers list of requests. The data usage is severely affected under such conditions, sometimes resulting in poor efficiencies. One solution to such a situation could be switching to a preferable network with less load and a much preferable bandwidth usage to the user's benefit. This ensures that load on the routers are effectively balanced, making connectivity easier and more effective [2].

Chapter 5

Data gathering for the system

We observed that the simplest Wi-Fi network is with only one AP. An AP located centrally in an enterprise or office environment was not our area of interest.

We tried to make an assessment about the real enterprise environment, but we couldn't make it. Unfortunately, no office or such places did not get convinced to provide us with their private data and to give us the chance to use their spaces and network infrastructure with the way we wanted.

So, with facing this obstacle we did try to make it in an alternative way, and we became able to make an assumption that reflects the real scenario as far as possible.

In one of our members' home, we made a mini enterprise environment. There we placed three routers which worked as three different APs with three different SSID's. For each AP, different numbers of smart-phone devices were designated.

Since these three APs range were overlapping and smart-phone devices were dynamically changing their positions within the different range of different APs, we saw how the distance, signal strength and channel frequency affect the APs Wi-Fi performance for the smart-phone devices regarding to its position.

5.1 Device connected to AP 1

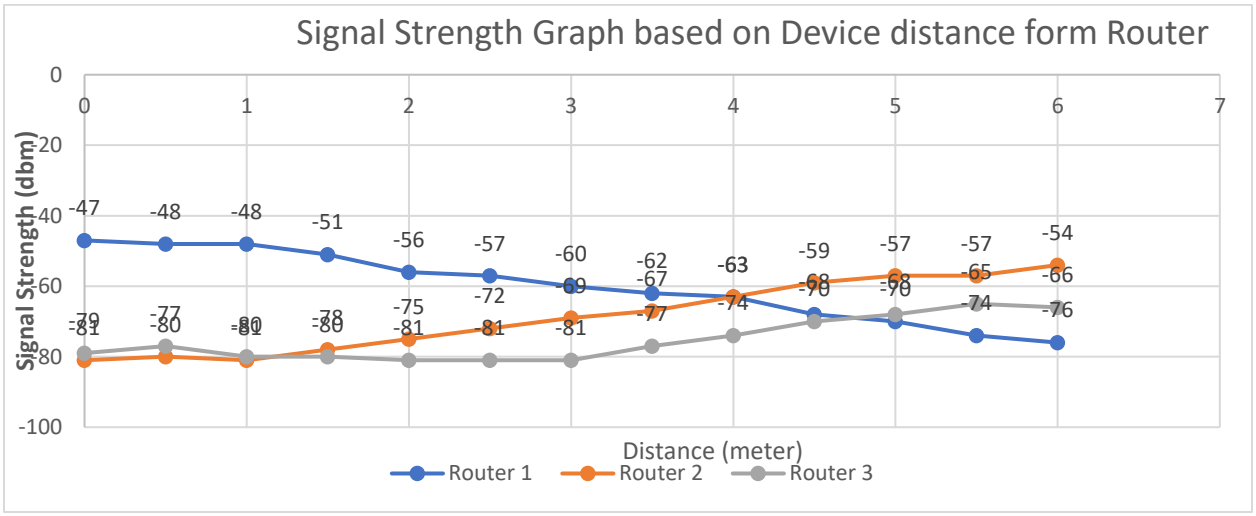


Figure 5.1: The graph while the device is connected to Router 1.

The graph above shows the real scenario for three different APs with overlapping range. This is the graph with the data of signal strength of three APs Router 1, Router 2 and Router 3 with different for different distances of a smart-phone from Router 1.

The line for Router 1 shows that when the distance increased, the signal strength decreased. It's natural. But other two lines, the lines for Router 2 and Router 3 trigger our interest. When the distances are in between 2.5 to 4 meters, the signal strengths are better from Router 2. And when the distances are in between from 3.5 to 6, the signal strengths are better from Router 3 for the smart-phone devices.

5.2 Device connected to AP 2

Same thing was shown by the APs when a smart-phone device was connected to Router 2 and was in different distances with Router 2.

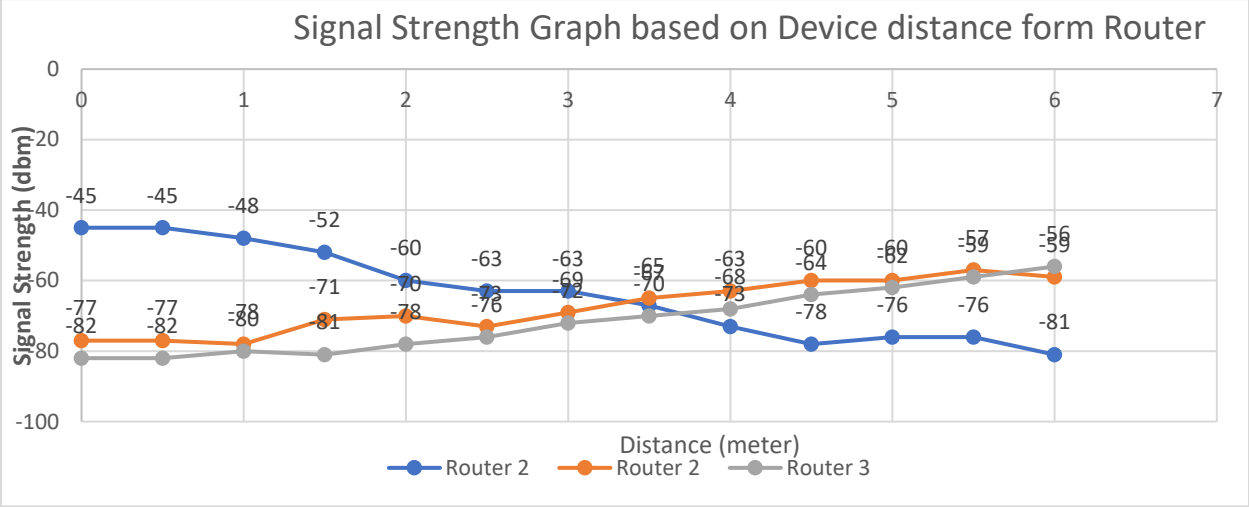


Figure 5.2: The graph while the device is connected to Router 2

Here, the line for Router 2 shows that the signal strengths were more intense when distances between the device and the Router 2 were 0 to 2.5. And when the distances increased, the signal strengths form Router 2 got weaker. For the distance in between 3 to 6 the signal strengths were more intense from other APs, Router 2 and Router 3.

So, the whole scenario indicates that the range of three APs overlapped. And this is quite natural for the enterprise environment. While moving, if the signal strengths from any AP are better than the signal strengths from the AP the device connected to, for most of the cases the AP with better signal strengths has potential of better internet performance.

But, only the signal strength is not the decision maker about the internet performance. Though signal strength is very much significant about internet speed, bandwidth and the channel the network using are also the key factors.

We worked on the scenario we described above and made an algorithm that will help in such scenarios of enterprise environment.

Chapter 6

Algorithm

As we stated earlier, our main goal is to generate an algorithm that makes the device automatically switch to the strongest network, more specifically, identify the access point (AP) with better performance and to connect with that. What makes our algorithm smart is the decision it makes to determine where to connect when multiple options exist. There is no need for the user to even think about this.

6.1 Algorithm Overview

Our algorithm has actually two portions. And two of them are constructed in a way that, both can technically work fine as an individual body. But we generated them to work together because only that way they can make real sense. For both portions of our algorithm, working as one body makes them practically attainable.

The Two portions are:

a) Achieve the access Algorithm
b) Establish the connection Algorithm

Our idea of the first portion, achieving the access Algorithm intersects with another research article. Somehow that helped us. The article named *'A Little Sharing Goes a Long Way: The Case for Reciprocal* Wi-Fi *Sharing'* found that for home APs there are opportunities for reciprocal Wi-Fi network sharing and it can be beneficial for the users who share their Wi-Fi network with others. For domestic scenario, Jinghao Shi, Liwen Gui, Dimitrios Koutsonikolas, Chunming Qiao and Geoffrey Challen, author of the article *'A Little Sharing Goes a Long Way: The Case for Reciprocal Wi-Fi Sharing'* stated [2] that the system should be able to control the sharing and the

access of home AP to other users, and revoking the access when needed. Another important thing is that the system should protect the home network from other users by sharing access only to the Internet, not to the other devices.

So, in the enterprise environment Wi-Fi network scenario, to get access to network through other APs, we considered two things: control and security. Achieving the access Algorithm works for those two things. With this algorithm, the device would be able to request for access to the internet by those APs it considers as neighbor networks, and can achieve the access. Since the neighbor networks also control the access, the password would not be necessary. As a result there is no chance that the security of any neighbor network can face any threat. Any ambiguity should not work there for any of the sides to make the system work.

This is only for the first portion of the algorithm.

The second portion of our algorithm, Establish the Connection Algorithm is actually the heart of the whole algorithm. This part makes decision when it would be wise to connect with another AP leaving its own AP and which AP is better to be connected with.

When this algorithm would be working, there are several things working behind the performance of a network. One of them can suggest to select the AP A and another one of them can suggest to be connected with the AP B. At that point, our algorithm makes comparison between the signal strength of different APs and interferences of channels used by those APs, and lastly connect with the better one.

6.1.1 Achieve the access Algorithm outline

1. There will be two categories for all the Wi-Fi signals or access points (AP). Only one AP will be selected to be in the category named ‘My Network’. And some other APs will be selected to be in the category named ‘Neighbor Networks’.
2. The device will be connected to the Home AP.
3. There are two methods. getOwnMac and keepInWhitelist.
4. getOwnMac method requests the device to return the device’s MAC address.

5. Through keepInWhitelist method, the device sends request to neighbor APs to add the device to their white lists.
6. The device gets the access to those APs without knowing the passwords of those APs.

6.1.2 Establish the connection Algorithm outline

1. The device will be connected to the 'Home AP', and the signal strength and bandwidth will be saved as variable.
2. There is an option named minimum signal strength. One will be chosen from given three options of signal strength (it can be -50dBm or -55dBm or -60dBm). It will work as the Threshold signal strength.
3. In every three minutes the signal strength will be checked.
4. If necessary, the goal is to find the AP with better network performance and make the Station connected with that AP.
5. Whether 'Home AP's signal strength is less than minimum signal strength (<-50dBm) or not? If yes, then it should find the APs with signal strengths of more than 'Home AP's signal strength from 'Neighbor APs'.
6. Organize those APs according to their signal strength.
7. Select the AP with highest signal strength and make a comparison between its bandwidth and lastly connected AP's bandwidth.
8. The bandwidth of AP with highest signal strength will be manipulated before comparison. (Bandwidth- 1.5kbps*0.35). This is for optimum network.
9. The network with greater bandwidth will be selected and device will switch. Other then, it won't.
10. When to select the channel then it should find out the AP using clearest channel.
11. Always some data will be saved in a buffer to prevent the packet missing and occurring error while the device changing its network.

6.2 Algorithm

System starts to work in every three minutes.

System starts{

// Home AP and neighbor AP will be selected differently

Wi-Fi signals = [HOME_AP_SSID, 1_SSID, 2_SSID,……..n_SSID] // all the signals showed in device

Home AP= {HOME_AP_SSID}

Neighbor APS= {1_SSID, 2_SSID, 3_SSID, 4_SSID}

AP current_AP= HOME_AP_SSID; // connected to Home AP

mac_addr= getOwnMac()

// method works

[getOwnMac(MAC){

MAC= MAC_address;

return MAC;

}]

keepInWhitelist();

[keepInWhitelist(MAC){

AP.access(MAC);

}]

// access

password= dummy_password;

```
//saving signal strength and bandwidth
current signal strength= Home_AP_signal_strength;
current bandwidth = Home_AP_bandwidth;
//threshold signal strength
Threshold strength = minimum signal strength;
If( current signal strength< threshold strength){
// system will find out another AP from Neighbor_APs category to be connected with.
} else {
// stay connected
}
AP ap_highest_signal_strength= Neighbor_APs {1_SSID, 2_SSID…..};
Current_ap= ap_highest_signal_strength;
If (current bandwidth=> last connected bandwidth-1.5 kbps*0.35 ){
// stay connect to this new AP
current_ap= new_AP_with_highest_Strength;
} else {
current_ao= 2nd_highest_signal_ap;
//system works on
}
// If two APs equally have the highest signal strength
```

```
            If (highest_signal_strength= = 1_SSID && 3_SSID){
                        current_ap= AP(clearest channel);
                    }
                //buffer
            Internet data= [] buffer;
        If (battery<=20%) {
            //System stops
        } else{
        }
}
```

6.3 System Overview

In enterprise environment, when the device's Wi-Fi option would be on, it would get signals from the several neighboring APs. The user knows which one is specific for him/her. And the user also should know which signals are from his/her enterprise.

Device will save that specific SSID in Home AP category, and will save the other SSIDs in Neighbor APs category.

Home AP= {HOME_AP_SSID}

Neighbor APS= {1_SSID, 2_SSID, 3_SSID, 4_SSID}

The device will stay connected to the {MY_AP_SSID}, with the authentication by the user with password.

As the system is working, it will request the device through the *getOwnMac* to return its MAC address.

```
getOwnMac(MAC){
        MAC= MAC_address;
        return MAC;
}
```

The system will request the neighboring users to authenticate for accessing through the keepInWhitelist () method. The neighboring users, who are sharing the system, will authenticate the request.

```
keepInWhitelist( MAC){
        Neighbor_ AP.access(MAC);
}
```

The users system will receive a notification about authentication. The system can finally get access to any neighbor network with a specific dummy password. This dummy password would be chosen by the user, user would never know the password of any neighbor network.

```
// access to 3_SSID
 password= dummy_password;
```

When the device is connected to the Home AP, the signal strength and bandwidth will be saved for later comparison.

```
//saving signal strength and bandwidth
 current signal strength= home_AP_signal_strength;
 current bandwidth = home_AP_bandwidth;
```

The user will select signal strength as minimum signal strength. Our assumption is that the user may not be fine with the technical representation of signal strength. So the user can select a distance that will work for minimum signal strength inside the system or the user can select the Wi-Fi signal strength symbol. For the system, this minimum signal strength will work as the threshold signal strength. When the device will cross this threshold strength for Home_AP, system will start to work for finding an AP with better internet performance. In every three minutes, system will check the current signal strength with threshold strength.

```
//threshold signal strength
Threshold strength = minimum signal strength;
If( current signal strength< threshold strength){
// system will find out another AP from Neighbor_APs category to be connected with.
} else {
// stay connected
}
```

System will select the AP with highest signal strength and will compare its bandwidth with the last connected AP's bandwidth, if the bandwidth is optimal, then it will stay to that AP, otherwise not.

```
If (current bandwidth=> last connected bandwidth-1.5 kbps*0.35 ){
// stay connect to this new AP
Current_ap= new_AP_with_highest_Strength;
} else {
Current_ap= 2nd_highest_signal_ap;
//system works on
}
```

```
If (highest_signal_strength= = 1_SSID && 3_SSID){
        current_ap= AP(clearest channel);
}
```

So, when the device crosses the minimum distance for threshold signal strength, the internet performance of that AP worsens, it would select the AP with highest signal strength and would give it the current status.

There can be a chance that this AP has enough signal strength, but it has no internet connection or very low bandwidth. To determine that the system will check its bandwidth.

If this AP's bandwidth is better than the last connected AP's bandwidth, that means the internet connection is okay.

If the signal strength is better, that doesn't necessarily mean that the bandwidth of this network is always better or greater than the last connected bandwidth. In that case, the system would get that the last connected AP has better speed and can connect with that, and that would work as a loop whole. To solve this, we used a function here. When system would compare the new AP bandwidth with the last connected bandwidth, it will use a function to decrease the last connected bandwidth. The decision making and switching will be so fast that it will not affect internet performance.

4. If, in any enterprise environment, multiple networks are being used by different APs, there obviously APs are using particular channel. And each network selects a channel that it tries avoid the overlapping of the channels. But for multiple networks within a fixed range, some interference occurs. So, when there is a circumstance that, two or more APs signal strength is highest and equal, and then it will select the AP/network using the clearest channel.

```
If (highest_signal_strength= = 1_SSID && 3_SSID){
```

```
            Current_AP= AP(clearest channel);

        }
```

Some internet data will always be saved in a buffer, it would help if any packet missing or error occur while changing the AP.

```
        //buffer

    Internet data= [] buffer;
```

6.4 Policies of Algorithm

We determine some policies for the algorithm we developed. Previously we already stated that we want to make the best use of the unlicensed spectrum of Wi-Fi system. Our vision is that such sharing will not remain only limited within one enterprise, such sharing will lead us toward the future where different organizations, companies, firms and institutions mutually share their Wi-Fi system satisfying their own interests and will be benefitted economically and technologically. Our system is attainable in real scenario with certain policies. Since our algorithm doesn't interfere the network infrastructure of any enterprise, the policies we determined are realistic and ensure the control and security of different APs and Wi-Fi system.

Our first policy is works for three things. They are mutual sharing, control and security. In a common enterprise, it is very much expected that the users of different APs will be interested in sharing. When the request of authenticate comes, it not only about to authenticate, it is about get authentication also. So, by sharing the APs, all of the users of an enterprise will get the same benefits. And the way algorithm works with the two methods getOwnMac() and keepInWhitelist() , they ensure the control and security. The users of Home_AP can control their device about the connection with neighbor APs. And with the second method the users of neighbor APs can ensure the security. Since the external users would not get the password of neighbor APs, they can't access to the other devices such as scanners, printers, TVs etc connected with the neighbor APs [2].

The user can select the minimum distance or minimum signal strength that would work as threshold strength. So, until the device crosses the specific distance, the system does not try to find out the AP with better performance. In this way, the system keeps the device away from unnecessary access to any neighbor AP. And it helps to not create unnecessary load on other AP. As the threshold strength minimizes the unnecessary calculation, it additionally helps to save the energy.

The third policy is totally about the energy efficiency. When the system is working and trying to make decision and ultimately switching the connection to AP, it consumes a significant amount of energy. So, to keep the system working all the time wouldn't be a wise thing. When the battery is equal or less than 20 percentage, the system will stop working.

Chapter 7

Implementation

We've built an android application to implement the system. Our Application is one of a kind. It's a complete package of Smart Wi-Fi Switching. Now a days Android Device is almost always connected with internet and without internet we can't go a single day. With being said about the importance of Handheld Device and always internet connectivity the overhead comes to our mind is about battery and the efficient way of Saving battery while keeping ourselves always connected with internet.

7.1 Application's work

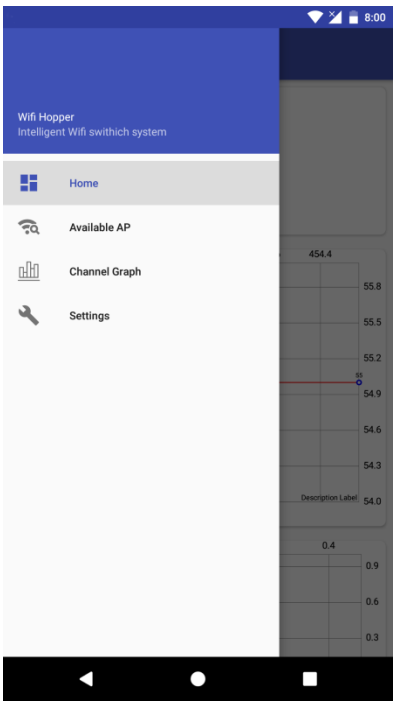


Figure 7.1: App navigation Menu

Users have to select and save the networks which user frequently want to get connected. These are the saved or paired list. Our Application will swap networks in between theses paired networks which we saved earlier.

Well it's worth repeating the algorithms main focus which is the application will swap between networks based on Primarily on Signal Strength, the frequency and also the best channel it can get. Getting connected into the network the first thing it will do is to save the current bandwidth in a temporary variable.

When the app swaps into a new network it will follow the same procedure but when the saved list has at least had two saved networks and also had the two bandwidths saved then will swap the network keeping the bandwidth along with the old parameters mentioned before.

So, in a nutshell our algorithm swaps users Wi-Fi network based on 4 parameters which are Signal Strength, Network Frequency, Best clear channel and the last saved bandwidth.

7.1.1 Home

Application will show connected router's SSID aka Network Name, BSSID aka MAC address, Signal Strength, Network Frequency and Connected Channel Number.

A line graph with markers will show the channel frequency graph with pointers showing the signal strengths.

A bandwidth graph (bar) will show the bandwidth of the current network which was previously stored under a variable will be shown in bar graph on instance of network speed and distance of the router and the device.

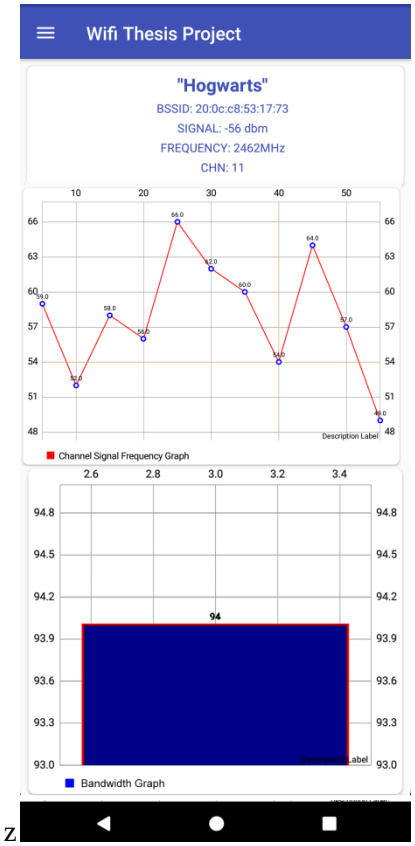


Figure 7.1.1: Home AP's current state

7.1.2 Available Access Points (AP)

Getting connected into Wi-Fi our application checks all the adjacent/ neighbor networks showing data related with the devices i.e. SSID, BSSID, UPTIME, Frequency, Signal Strength, and Channel. It will only show the neighbor networks whether they are paired or not.

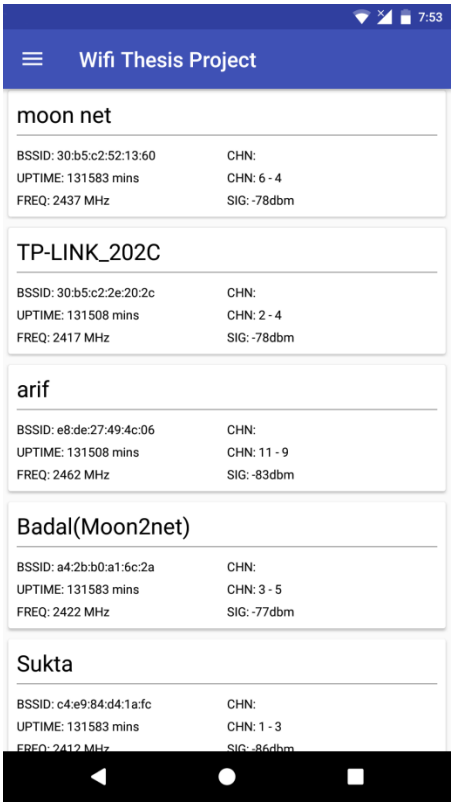


Figure 7.1.2: Neighbor AP's Information

7.1.3 Channel Frequency Rating

There will be few graphs based on the Wi-Fi channel numbers and their related data to be precise the signal strength and their distance form router to handheld device. These graphs will show the line graphs with the pointers which is the signal strength.

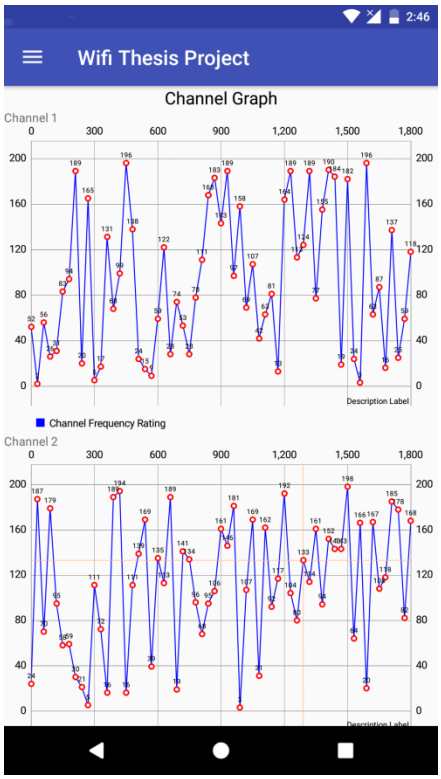


Figure 7.1.3: Channel graph

7.2 Outcome and analysis

The features of our application already explained what this simple yet robust application can do. Well we are going to point and sort out all the advantages the app will give a user in daily use.

Suppose you are in an office environment and it has more than one Wi-Fi router and you are paired with all of them but usually you are connected with one of the router which you get connected first when you enter into the office.

Well you will face network problem definitely as you will move rooms to rooms for office work purpose, maybe you will go to lobby for some reasons, maybe there are many users connected with the same router and all are using internet in the same time, maybe someone is downloading or streaming videos.

So, what will happen is, you will face hindrance in internet using and what is the solution of that? Does your default android system provide you to switch the network automatically?

The answer is NO. The system Wi-Fi algorithm will keep you connected to that particular Wi-Fi unless and until it completely loses its connection. I guess we all have seen in android that Wi-Fi is connected in low signal strength and you are connected but can't able to surf in the net.

Here are some simulation based graphical reports we have created mentioning different parameters. The simulations are based on network signal strength, network frequency, distance form handheld device and router.

Device	Distance	Strength
Hogwarts	0	-55
	50	-55
	100	-58
	150	-59
	200	-62
	250	-60
	300	-59
UB40404	350	-63
	400	-65
	450	-62
	500	-67
	550	-72
	600	-72

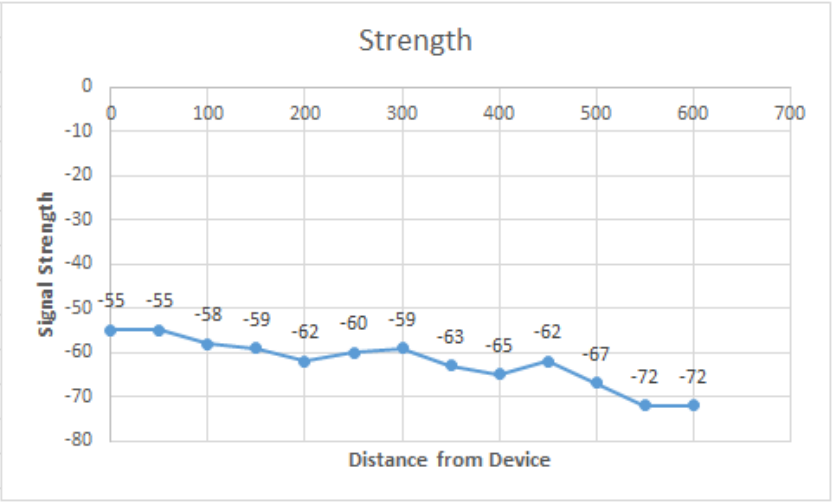


Fig: Graphical simulation based on distance and Signal Strength

Device	Distance	Device Location
Hogwarts	0	
UB40404	574	
UB40303	85	The
UB40402	366	device
UB40203	443	is
UB40301	60	at
UB40401	428	3rd
UB30304	185	Floor
UB40303	165	of
UB40301	25	UB4
UB40203	550	

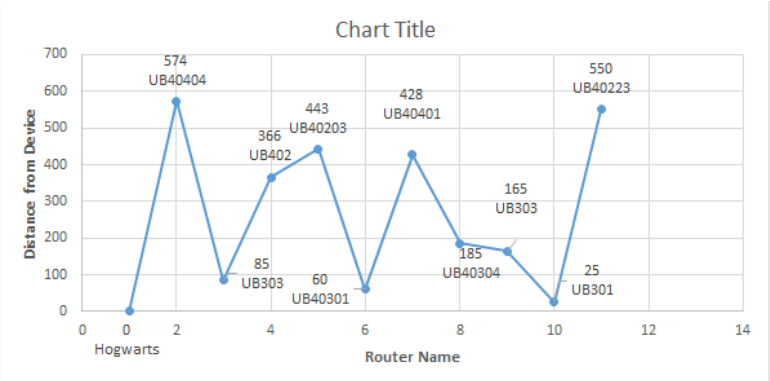


Fig: Graphical simulation based on Router Signal Strength from a Specific Point

Our application is mainly made keeping in mind about the enterprise Internet usage. No further ado let's see the advantages:

1. App will automatically switch users to better Wi-Fi network.
2. If the Wi-Fi is connected but there is no internet it will swap the user to next best network with higher preferences.
3. If a router has many users and the bandwidth drain is major the app will connect the device to the router and as soon as it connects it can measure the current bandwidth and automatically swap to the next best one.
4. App Service will automatically Turn off the service if the battery level is below 15%
5. App will turn off the Wi-Fi if the user is not connected to any router for more than 30 minutes.
6. Service will always run in background.
7. User can always check the Graphs to understand the connected network status and its network status.

8. It will make the enterprise usage of Wi-Fi more easily and as it swaps seamlessly the user will never face disruption of Internet and will never miss any updates, calls, notifications.

It is said earlier that Android OS has some constrains and it can't be in done without root access. So here are some solutions or issue we overcame across building the application:

1. We are giving a Message (toast) if the Android OS in not asking for Location Permission. It will let the user know that s/he have to turn the location service on.
2. As said earlier that location service consumes battery life and our App needs location service to be turned on. So, we came up with a solution; which is user can set the Location Service to "Battery Save" mode and it will keep the battery healthy and make the App run.

Chapter 8

Conclusion

If we notice the urban environment we live, we can see that how fast the usage of Wi-Fi is increasing. It can be home or working place, when we switch on Wi-Fi option of our device, we get signals from a significant number of Wi-Fi networks. There are some drawbacks of our application. Well as we are using only the handheld device and using Android as the Operating System, naturally it comes with some constrains of its own. There are some options to solve some issues but it needs root access of the user's Android device. Which is unlike to happen as Android OS never gives the root access without any tweak in their ROM and Kernel.

8.1 Limitations

We tried our level best to overcome and fix some issues but some are too stubborn to fix. Here are the disadvantages a user may face while using our Application:

1. App is only Android based so it gets the best network based on the Device Antenna quality. Low budget handsets come with poor quality antenna and it can never able to receive the best Signal of a router.
2. App needs Location Permission to Access and get information of the adjacent networks. Without the location permission given it can't perform the service.
    a. Android 6.0~7.0 ask for the permission for the app when user opens the application
    b. Lower versions on Android Application do not ask for the permission and it never able to run the service. So, user have to turn the location manually.
3. Location Service Consumes battery life than more than usual.

4. When the Application Swapping service is turned on it consumes more battery as it had to check and swap between networks.

8.2 Future Work

It is important that, our system and algorithm have the potential to be developed to work for other devices other than smart-phone and other technology other than Wi-Fi.

As far as we have come, we can see that there are further possibilities to develop this algorithm and to apply it for more purposes.

1. To make it workable for other devices and operating systems other than smart-phone and android.
2. This algorithm has potential to work for load balancing of the access points (AP).
3. Another function can be added to this algorithm for comparison of different cellular networks and Wi-Fi network.

Our algorithm now works for smart-phone devices. And we implemented it for android based devices. As we developed this system considering that the device would move and the distance with the AP increases, that makes us to face the reality of sharing. So, the system is easily attainable for other smart-phone other than android based. And with the concept, it is also attainable for laptop. And for that the system should be implemented to be compatible with the operating systems of computer. If this happens, then it can also work in desktop computer for the VLAN system.

One of our future targets is make our system work efficiently for the load balancing of access point (AP). If the system can be developed to work in network infrastructure level of home or enterprise environment, it will be able to control the AP and its users. Now, in our system, the load balancing is possible with a bit inefficient way. If the system compare the number of users connected with the APs, it will cause more switching. If it would be possible to determine the number of users connected to an AP without being connected to that AP, it would help.

It is highly interesting that we want to develop our algorithm to meet a specific purpose to select from different kind of networks [11]. We believe, in future, for smart-phone and such devices our developed system will be able to make a decision about cellular network of different types such as 2G, 3G and 4G, and can compare with Wi-Fi network.

8.3 Conclusion

We think, in future, the reality of Wi-Fi will be that every organization and individual will believe in mutual sharing and the sharing will satisfy their mutual interests. We believe, our algorithm and system have the potential to lead us in the future where the sharing will occur not only within the APs, but among the different Wi-Fi networks of different organizations and individuals. For that, we have to think forward and realize that this sharing is not a zero-sum game. In summary, our algorithm and its deployment is about the immense economic and technological benefits of unlicensed spectrum, it works for development of Wi-Fi system in enterprise environment.

REFERENCES

[1] Piotr Gawłowicz, Sven Zehl, Anatolij Zubow, Adam Wolisz. Jul 2016. NxWLAN: Neighborhood eXtensible WLAN.

[2] J. Shi, L. Gui, D. Koutsonikolas, C. Qiao, and G. Challen, "A little sharing goes a long way: The case for reciprocal wifi sharing," in Proceedings of the 2nd International Workshop on Hot Topics in Wireless. ACM, 2015.

[3] S. Zehl, A. Zubow, M. Döring, and A. Wolisz, "ResFi: A Secure Framework for Self Organized Radio Resource Management in Residential WiFi Networks," in 17th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2016, June 2016.

[4] A. Zubow, S. Zehl, and A. Wolisz, "BIG AP – Seamless Handover in High Performance Enterprise IEEE 802.11 Networks," in Network Operations and Management Symposium (NOMS), 2016 IEEE, April 2016.

[5] Y. Yiakoumis, M. Bansal, S. Katti, and N. McKeown, "Sdn for dense wifi networks," Presented as part of the Open Networking Summit 2014 (ONS 2014), 2014.

[6] J. Schulz-Zander, N. Sarrar, and S. Schmid, "Aeroflux: A near-sighted controller architecture for software-defined wireless networks," in Presented as part of the Open Networking Summit 2014 (ONS 2014), 2014.

[7] Open Wireless Movement. https://openwireless.org/.

[8] why-do-wifi-connection-speeds-keep-changing. https://www.lifewire.com/

[9] everything-you-need-know-about-android-and-wifi. http://www.androidcentral.com

[10] bandwidth-vs-signal-strength-how-to-get-the-best-internet-connection-for-your-device. http://www.zdnet.com/

[11] Nirjon, S., Nicoara, A., Hsu, C.-H., Singh, J. P., and Stankovic, J. A. Multinets: A system for real-time switching between multiple network interfaces on mobile devices. ACM Transactions on Embedded Computing Systems (TECS) 13, 4s (2014), 121.

[12] J. Shi, L. Meng, A. Striegel, C, Qiao, D. Koutsonikolas and G. Challen. "A Walk on the Client Side: Monitoring Enterprise Wifi Networks Using Smartphone Channel Scans". In Proceedings of INFOCOM'16, 2016.

[13] technical_factors_affecting_wireless_performance. http://www.4gon.co.uk/solutions.

[14] how-to-boost-your-wifi-speed-by-choosing-the-right-channel. https://www.extremetech.com

[15] what-is-wifi-and-how-does-it-work. http://ccm.net