The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

Enhanced Link Layer Handover Based on Localization

Prepared by: Xola Kumbuza Supervised by: Neco Ventura

May 30, 2008

University of Cape Town

This thesis is submitted in accordance with the requirements of the University of Cape Town (UCT) for the degree of Master of Science.

I declare that this dissertation is my own work. Work used which is generated by other research is noted and included in the references. This work has not been submitted before for any degree or examination in any other university.

Signature of author
Date
Xola Kumbuza

University of Cape Town

Abstract

Wireless Technologies over the past years have become cheaper and more available to users. In the Infrastructure Mode of operation, when a mobile node moves from the coverage of one Access Point (AP) to the coverage of another AP, it is said to undergo handoff. The mobile node has to complete a link layer handoff together with other tasks associated with handoff in order to effectively have a new wireless link with the new AP. The link layer handoff currently specified and practiced in IEEE 802.11 is normally carried out in three time steps. These are; the Scanning Phase; the Authentication Phase and the Association Phase. During the three steps the mobile node is unable to send or receive data meaning that packets are lost or delayed causing real-time applications such as video streaming or VoIP, which can only tolerate an end-to-end delay of 50 ms during handoff, to suffer.

The Scanning phase can be done passively or actively. In passive scanning, the mobile node listens on every bandwidth channel for Beacon Frames from the APs. In active scanning, the mobile node sends Probe Requests frames on every channel expecting to receive Probe Responses from the APs operating on each channel.

Localization is the process of a node finding its position in space. Localization methods include the Global Positioning Service (GPS), Cricket, Ultrasonic Location and many more. This study investigates how localization can be used to decrease the latency delay experienced at the link layer during wireless handoff. In our method, a mobile node is given the ability to have knowledge of the APs through an AP-Table server. The mobile node then uses localization to find the closest APs to it and make faster, smarter handoffs.

Our simulations are implemented using the NCTUns network simulator and emulator. The simulations comprise of a mobile node undergoing handoff between APs in the same subnet and APs in different subnets. Added to that, the direction of the mobile node is monitored and used to further assist the handoff process to alleviate the number of total handoffs.

Our research shows the disadvantages and advantages of the proposed system as it integrates localization and direction into WLAN and mobile communication.

University of Cape Town

Acknowledgments

I wish to thank the following individuals and teams for the support some of which stretches beyond the period during which this thesis was carried out.

- Mr. Neco Ventura, my supervisor for inviting me to do masters and encouraging me to work hard and finish.
- Telkom and the NRF for giving the financial backing that helped me achieve what I have achieved at Masters level, and especially Mr. David Browne for guiding me in specific areas that channelled my thesis. I look forward to working for Telkom
- Vitalis Ozianyi and Benon Muwonge who are friends and colleagues studying postgraduate studies at the University of Cape Town, for all the help and support.
- The University of Taiwan, for providing the software, and providing guidance especially in the early stages of my simulations. From this university I would especially like to thank C.C Lin and C.L Chou for their assistance.
- My parents, siblings and extended family for being the most influential people in my life, for all the support, love and encouragement that you have given me throughout my life.
- My friends in Cape Town and beyond, the UCT Engineering staff, all those who helped me to go to the conference at the University of Michigan in May of 2006.
- Prof. Gaunt, the Head of Department Electrical Engineering, the Administrative Staff Electrical Engineering.

University of Cape Town

Contents

University of Cape Town

University of Cape Town

List of Figures

University of Cape Town

List of Tables

University of Cape Town

Chapter 1

Introduction

University of Cape Town

1.1 Background Information

The miniaturization of Information Technology (IT) devices and growth of wireless communication has led to a need for mobility solutions and hence the increase of wireless and mobile communications research. IEEE 802.11 Wireless Local Area Networks (WLANs) have also experienced growth leading to the establishment of different 802.11x standards such as 802.11a, 802.11b, 802.11e, etc.

WLAN has two operational modes known as the ad-hoc and infrastructure mode. In ad-hoc mode, mobile nodes communicate in a peer-to-peer way while in Infrastructure mode mobile nodes get access to a network through Access Points (APs). Due to the fact that in infrastructure mode an AP connects mobile nodes to the network, APs normally have a wired connection to an Access Router (AR) that connects them to the network. In 802.11b, the wireless link between the AP and the mobile node uses radio frequency waves that operate in a partitioned 2.4 GHz frequency band. A wireless device with WLAN capability can then access one of the partitioned bands (also known as a frequency channel) at a time in order to gain access to the network. The partitioned frequency bands in 802.11b are normally divided into eleven operating frequency channels within the 2.4 GHz band. In order to avoid frequency interference during operation, the operating channel frequency of neighbouring APs is normally set as far apart as possible. When a mobile node connects to an AP, they both communicate in the same frequency channel. However as the mobile node moves away from an AP, it experiences a degradation in connection because the strength of a radio frequency coverage of an AP weakens as one moves away from it. This can also happen if the mobile node loses line of sight with the current AP due to obstructing objects. This poses a problem to users who expect to have connectivity at all times even when they are mobile. To extend the coverage of infrastructure mode, multiple APs can be established in an area so that when the mobile node moves out of coverage of one AP, it moves into the coverage of another. This means that the mobile node must communicate with different APs at different times to access the network during its movement. When a mobile node accesses the network via a new AP, it tunes into the new frequency channel being used by that new AP. A mobile node can move from one AP to another AP that is connected to the same AR (micro-mobility) or to an AP that is connected to a different AR (macro-mobility).

The Internet Engineering Task Force (IETF) proposed the Mobile Internet Protocol (MIP) as the supporting structure for this phenomenon of a mobile node changing APs. MIP aims to connect a mobile node from one AP to another without losing any ongoing sessions of the mobile node. When this happens, the mobile node is said to undergo a handoff or handover. In the process of handover, a mobile node must first detect that it can no longer get acceptable service from the current AP, and then begin a link layer or 802.11 handoff, which scans all frequency channels of 802.11b and associates to a new AP. The mobile node can use active or passive scanning to detect the presence of other reachable 802.11b APs. As depicted in figure 1.1, in active scanning, the mobile node sends probe request frames on every channel; the APs would reply to these with probe responses. In passive scanning, the mobile node periodically listens on each channel for beacons in order to choose the best AP. With the information gathered from probe responses or beacons, the mobile node normally makes a decision of the next AP based on the Signal-to-Noise Ratio (SNR) and proceeds to authenticate and associate with it. In figure 1.1, the mobile node scans all the channels and only associates to AP10 in channel 11. From this, it is evident that there is a lot of signalling and time wasted in the scanning phase of the link layer or 802.11 handoff.

University of Cape Town

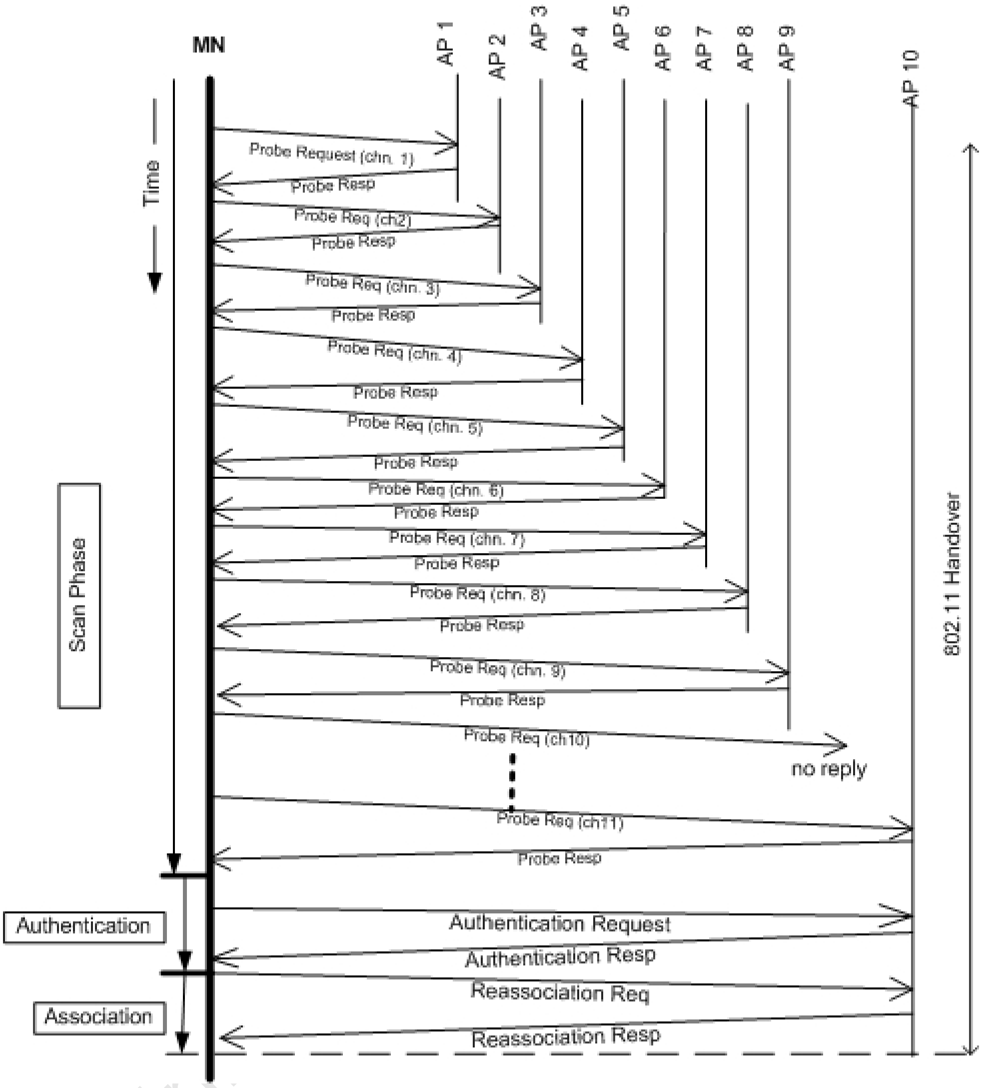


Figure 1.1: Signalling involved during Link Layer Handoff

The scanning phase of link layer handoff normally takes about 90% of the total time required to associate to an AP [4, 5]. This contributes to the time that the mobile node takes to complete a MIP handoff and results in perceivable degradation in the quality of real-time sensitive data such as Voice over IP (VoIP). Real-time sensitive data can normally tolerate only a maximum end-to-end delay of 50ms [5]. A more detailed description of MIP is given in Appendix E.

The current technique of scanning all channels is unable to always achieve optimum latencies. Therefore to obtain optimum latencies, research in this area of handoff has suggested both the reduction of channels to scan as well as algorithms to reduce the number of APs to scan. The Channel Mapping Scheme [25] and Neighbour Graph algorithms [5] are examples of such methods. While the Channel Mapping Scheme focuses mainly on reducing the channels scanned, Neighbour Graph algorithms focus on establishing a relationship between adjacent APs so that the mobile node can scan for those APs. It is also possible to improve link layer scanning latency by scanning for new APs while the mobile node is connected to the current AP. Examples of these include the Multiscan [9] and SyncScan [22] techniques.

MultiScan [9] reduces the effective scanning time to zero seconds by utilising two wireless network cards to complete handoffs. The card known as the primary card is the one which would be connected to an AP whilst the other card known as the secondary card is free to scan other frequency channels [9]. The problem of MultiScan is that it suffers from interference because both cards operate around the same frequency (i.e. 2.4GHz).

SyncScan [22] performs a similar function to MultiScan but it uses only one card and periodically scans all channels while being serviced by the current AP. The APs of a particular channel are synchronised to transmit their beacons at a time when the mobile node switches to listen on that channel. In this way, the mobile node ends up having an up-to-date list of reachable APs around it. It does this while managing to replace the large transient overhead of normal full scanning. However, the channel switching can cause disruption and some data loss. A synchronization problem also develops over long periods of time [6].

Other handover enhancement proposals, rely on predicting the movement of mobile nodes by considering the movement history of the node. This method of predicting the movement of a mobile node is known as the deep mining technique. Deep Mining techniques however assume that a mobile node will always move in a certain direction in accordance to its history. In addition, if the historic movement of a node is unknown, then movement prediction will not succeed as a mobility enhancement tool. Added to that, even though the movement history of a mobile node can be effective for mobility management, it depends on a learning algorithm that needs many handoffs in order to become effective as a mobility enhancement tool. Wijngaert et al. [8] for example proposed a location management technique that uses movement prediction where the mobile node moves in a trajectory that is known beforehand to make handoff to the nearest AP. Distance calculation is used to induce the triggers that are unavailable in 802.11b to carry out Pre-Registration or Post-Registration. By extrapolating a list of the next likely APs in the mobile nodes trajectory, a large part of the handoff signalling is done in advance to the mobile node arriving at the AP. Wijngaert et al. further enhanced their model with the Urban Mobility Model that is not dependant on knowing the trajectory of the mobile node. In this system, the nodes move on actual street data extracted from Geographical Information System (GIS) databases. Parameters such as weight, width, directions,

University of Cape Town

speed, pause time, and position coordinates characterise each street data. The street data is parsed to a weighted directed graph and the mobile node can then use this data in different movement modes such as Random Intersection, Target Flags, and Random Next Hop to determine whether it is in line of site and to choose which AP to handoff to next. The focus however is more on integrating location systems into the Pre-Registration protocol, which is a layer three protocol, and there is no reference made to improving scanning at the link layer level.

This research proposes the use of location management or localization as a tool for minimising scanning during link layer handover. The problem is that most handover solutions are mainly topological yet a mobile node moves geographically as well. Taking geographical movement of mobile node into account has advantages such as:

- by considering direction and coordinates, a mobile node can have a more robust way of detecting movement towards and away from APs.
- a mobile node would have an alternative method to check a connection to an AP, using distance as well as the expected SNR to validate that the AP is within or out of reach .
- if location management coupled with prediction algorithms such as Deep Mining is incorporated in handover, then the mobile node will be more aware of its path to an AP over time.
- In more advanced systems, knowing the next AP by calculating the distance to it can trigger resource reservation and aid upper layer process such as the establishment of context transfers at the next AP.

In our system, the locations of APs along with other characteristics such as SNR are stored in an accessible table at a server called the AP-Table server. All APs have a wired connection to the AP-Table server. The APs upload their characteristics to this AP-Table server. A mobile node is able to get the locations and features of these APs through accessing the AP-Table server via the current AP (since that AP would have a wired connection to the AP-Table server). Through the localization tool, the mobile node can determine its own location and then use the information from the AP-Table server to calculate the actual SNR from each AP. This would then allow the mobile node to have an idea of how effective each APs coverage will be in relation to its position.

Examples of localization techniques include the Global Positioning System (GPS). Mobile devices with GPS transceiver capabilities can use GPS to find their location, velocity, direction and time in the world [2]. Communication satellites orbiting the earth are a free resource that is utilised in GPS. In today's high tech world, GPS transceivers are small enough to fit into mobile

University of Cape Town

nodes such as laptops [2, 3]. Although currently, GPS transceivers are fitted into mobile nodes for other useful functions that are not related to mobility in 802.11b, this research shows that GPS and other localization techniques can be incorporated to assist as a location tool to enhances handovers.

The usage of localization is proposed to be backwards compatible to the normal link layer scanning scheme, so that in areas where perhaps localization is not possible such as when GPS signals are blocked by buildings, the system can still be able to function using the default way of scanning.

Localization as a tool that aids at link layer handoff can be useful in situations where:

- Priority mobile nodes working remotely can use location-aided handoff as a way to improve real time communication.
- Vehicles streaming real-time data (e.g. video conferencing in a car) can roam anywhere in a city or outside of a city and still have good service by using localization systems that aid in link layer handoff.
- Mobile nodes Streaming from trains can also use location-aided handoff to have consistently low latency link layer handoffs.

While GPS is applicable for outdoor communication, it is not applicable indoors. An account of indoor localization methods can be found in Appendix B. These include Cricket, the Active Badge System, Ultrasonic location and The Augment Reality Technique.

1.2 Problem Description

The WLAN standard uses hard handover or a break-before-make method to find APs. When a mobile node connected to one WLAN AP wants to connect to another, it must first break the link that it has with the current AP before scanning for another one. The current method employed in 802.11b for finding a new AP by scanning all frequency channels takes too long and utilises a lot of signalling. This often contributes to a mobile node experiencing noticeable delays and packet loss when receiving real-time traffic during this time.

One of the best proposed solutions for this problem has been the MultiScan technique but it inherently has a problem of frequency interference, since it uses two wireless cards that access frequency channel that are very close to each other.

With the advent of the incorporation of location management tools into mobile nodes, there are possibilities of using these tools to obtain optimum handoffs where there's less scanning. This is the goal of this research: to have a solution that will satisfy real-time traffic by taking a maximum time of 50 ms or less to complete link layer handoff.

University of Cape Town

1.3 Thesis Objectives

This study investigates methods for the quickest ways of finding the next best AP for a mobile node. The focus of the research is at the link layer. The investigation integrates location management with link layer handoff and is conducted using software simulations. These simulations evaluate whether the usage of location management can speed up a mobile node finding and associating to the next best AP at the link layer level.

The study highlights the disadvantages and advantages of the proposed system and its incorporation into WLAN and mobile communications. This research also shows that using location management and direction can result in a mobile node making the least possible number of handoffs upon reaching its destination.

1.4 Scope and Limitations

In order to carry out the project, collaboration between localization technology such as GPS and link layer handoff is essential. This thesis only investigates layer two mobility aspects of 802.11b. The simulations done in this research compare normal active full scanning with methods that enforce selective scanning. The research only aims to lessen the time taken by a mobile node to find and be associated to an AP. This research does not aim to improve localization techniques. Localization can be done in an indoor or an outdoor environment, but our simulations focus on outdoor localization. The simulations done assume that the localization technique has no inaccuracies. In this way, the blockages that would create positional inaccuracies when the mobile node communicates with the GPS system is not simulated. The effect of obstacles on the system is however not included in the scope of our simulations, but as further work that would require new research study.

The speed of the mobile node is also kept at a low constant. This means that we do not simulate the effect of speed on our algorithms. This is because speed is more useful as a tool for predicting when loss of connection to the current AP will occur and thus reserving resources and communicating with the AP so that it could forward data to the new AP accordingly and thus ensure minimum data losses [43]. For this reason, the speed of a mobile node does not play an important role in minimising layer two latency times.

Our research considers only horizontal handoffs between homogeneous 802.11 WLANs. Vertical handoffs such as those between 802.11 and General Packet Radio Service (GPRS) are not considered.

1.5 Thesis Outline

The structure of the thesis is as follows:

University of Cape Town

- Chapter 2 focuses on the literature review that is relevant to the work done. Various other scanning techniques are explained in order to emphasise their usefulness and their shortcomings. The relevance of our research to these other scanning techniques is given. In this chapter, indoor and outdoor location management techniques are discussed.

- Chapter 3 serves to describe our proposed system and its operation. The integration of localization and its role in 802.11b handover is described. Unimplemented parts of the architecture proposed are outlined.

- Chapter 4 presents the simulation scenarios used to evaluate our system. A diagrammatic model is given along with an explanation of how the simulation functions and the parameter to be recorded for each simulation.

- Chapter 5 shows results obtained in our simulations. An analysis of these results in comparison with results presented in related works is presented before the recommendations are given.

- In Chapter 6, recommendations of ways to improve the proposed schemes are presented.

University of Cape Town

Chapter 2

Related Work

University of Cape Town

This chapter gives an overview of layer two mobility in WLANs. A detailed description of 802.11b highlights the handoff latency that occurs at layer two. Although different events might occur at upper layers when a mobile node is undergoing handoff, the same events happen at layer two; the mobile node has to do a layer two scan in order to find the next AP. The IEEE 802.11b is a Medium Access Control (MAC) protocol that facilitates this scanning procedure.

An understanding of the 802.11b protocol is therefore crucial for the development of suitable handover solutions [8, 15, 18]. A deeper understanding of the steps involved at layer two are given in this chapter in order to highlight the relevance and focus of our study. This will also explain the role of localization in the research and how it will be fused with layer two processes to create a workable low latency handoff scheme. Some previous studies which have tried to achieve the same goal of our thesis will be mentioned according to their relevance to this research, whilst other general techniques for minimising layer two latency handoff have been placed in Appendix A.

Since our solution depends on the mobile node knowing its position, a chosen localization tool in the form of GPS will be explained, whilst other localization techniques have been made available in Appendix B.

In chapter three, our solution which dictates that the mobile node make clever handoff decisions based on surrounding AP signal strength, will be fully described. The entities used along with the metrics to be measured will be described and explained.

2.1 IEEE 802.11b

IEEE 802.11b is a break-before-make protocol for linking wireless nodes. There are a number of standards of 802.11 [13], but in this study we focus on 802.11b, which is the most commonly used [4]. 802.11b is a MAC protocol that operates on the 2.4GHz frequency band and supports data rates of up

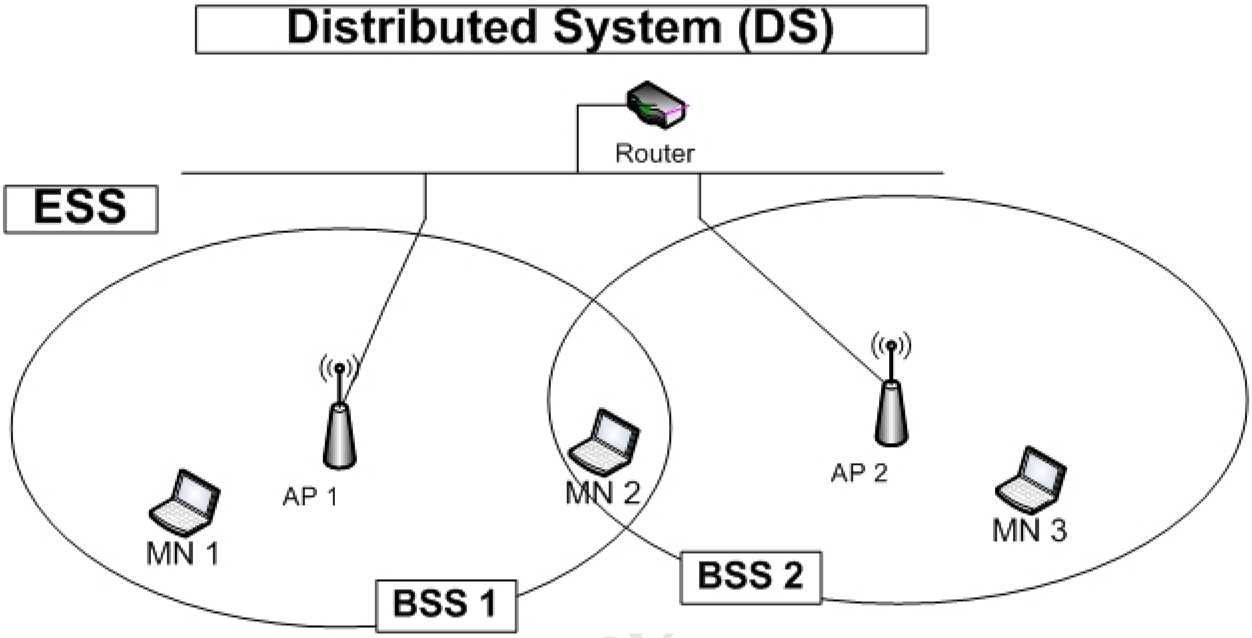


Figure 2.1: A Distributed System

University of Cape

to 11Mbps. It supports three types of network topologies: the Independent Basic Service Set (IBSS), commonly known as the Ad-hoc mode, the Basic Service Set (BSS) and the Extended Service Set (ESS), which are commonly referred to as the Infrastructure mode. A typical BSS is shown in Figure 2.1. BSSs that belong to one Access Router (AR) form an ESS. Figure 2.1 shows two BSSs that are linked to form a sub- or distributed-network.

In the above figure, MN 1 would connect to the network via AP 1, and MN 3 would get access to the network through AP 2. MN 2 is in the coverage of both APs hence it would choose one AP to get access to the network. The mobile node would make a decision based on which AP has the best signal strength. After choosing one of the APs, it then authenticates itself to that AP using the Open-System Authentication or a Shared Key Authentication [17]. The Open-System method consists of a 2-way null message exchange between the mobile node and the AP. The Shared Key method, involves a shared secret key to authenticate the mobile node to the AP. After authentication, association of the mobile node to the AP begins with the mobile node sending an Association Request frame (or Re-association if the mobile node is already associated) to the AP, and the AP replying with the appropriate Association (or Re-association) Reply. Although authentication and association are layer two functions, they do not take as much time as the link layer scanning in 802.11b networks.

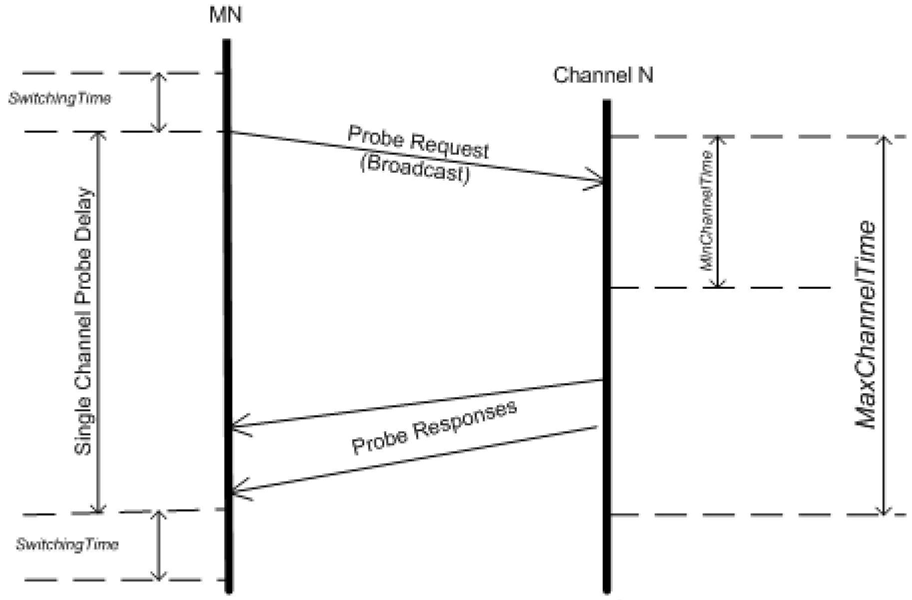


Figure 2.2: How a single channel is scanned

2.2 Link Layer Scanning

When a mobile node moves out of the coverage of its current AP, it begins a link layer scan to try to detect other reachable APs. Two scanning strategies can be used to detect the presence of APs. These are active and passive scanning. In active scanning, the mobile node sends Probe Request frames on every channel; the APs reply to these with Probe Responses. The mobile node receives the Probe Responses and creates an up-to-date list of available APs and their signal strengths. In passive scanning, the mobile node listens in each channel for beacons for a certain period in order to create the list of APs. A beacon is an advertisement that is continuously sent by an AP to enable mobile nodes within its coverage to learn about its presence. An AP typically sends beacons every 100 ms. Apart from sending beacons periodically, an AP also sends them as a response when it receives a Probe Request.

When a mobile node loses connectivity with the current AP, it would do a frequency change to a new channel and then wait for a minimum period called *MinChannelTime*. The *MinChannelTime* is the least time that the mobile node should spend in the frequency channel slot to find out if the channel is busy. If the channel is not busy, the mobile node will move to the next channel. If the channel is busy, the mobile node will wait until *MaxChannelTime* before moving to the next channel so as to receive any Probe Responses that might have been sent by APs operating in that channel.

As shown in figure 2.2 the frequency change to a new channel by a mo-

University of Cape

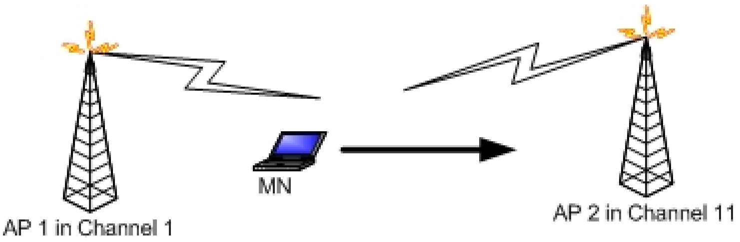


Figure 2.3: A mobile node and two APs in different channels

bile node is known as the Switching Time. The latency introduced by the Switching Time varies between mobile nodes of different vendors and for this reason, the Switching Time will not be modelled. For example, an Atheros based Network Interface Card (NIC) has a SwitchingTime of 5ms, meaning that the total delay involved becomes 10ms plus the single channel probe delay or *MaxChannelTime*. Because the 802.11 protocol does not dictate the values, the time allocation of *MinChannelTime* and *MaxChannelTime* is normally left up to the manufacturers [29]. Different researchers have suggested ideal settings for *MinChannelTime* ranging from 1ms to 7ms while the ideal *MaxChannelTime* has been suggested to be roughly 11ms [4, 22, 29]. These values have not been modelled here because they are out of scope of the study and are altered at the vendors choice. Once all the channels have been scanned, the mobile node will have a list of all the Probe Responses of every available AP and their signal strength. The mobile node will then make a decision on the AP to handoff to by choosing the AP with the best Received Signal Strength Indicator (RSSI) received.

Active scanning is said to be pre-emptive because it attempts to find the network whereas passive scanning is non pre-emptive since it waits for the network to announce itself [16]. Figure 2.3 shows a mobile node attached to an AP in channel 1 that needs to handoff to another AP that is in channel 11. The mobile node will iterate through all the channels from 1 to 11 in passive or active scanning in order to collect Probe Responses in each of the channels.

This current way of scanning leads to a problem because the mobile node would scan all channels, even those that are empty, only to choose one AP in a particular channel. Thus resulting in the scanning procedure greatly contributing to the link layer handoff delay. In passive scanning the scanning time normally takes 1.1s when the beacon interval of the APs is set to 100ms [25], whereas in active scanning, scanning can take up to and above 450 ms [25]. Active scanning is faster, but consumes slightly more power in comparison to passive scanning [24]. On the other hand, passive scanning takes too much time (i.e. $>$ 1 s), which can adversely affect real-time traffic delivery to the mobile node.

University of Cape Town

2.3 Selective Scanning vs Full Scanning

The most used methods of scanning frequency channels in 802.11b is the one described in section 2.2 above. These scanning methods are both examples of Full scanning. This is because in both methods, the mobile node has to visit each available channel in 802.11b when scanning. There has been proposals by researchers to optimise layer two scanning by reducing the number of channels to scan, or the number of APs to scan within a channel [6, 5, 14]. This process is called Selective Scanning and is a process which is adopted by our research. Other research has suggested other ways which require hardware changes to the mobile nodes and/or APs [22, 9]. These alternative methods have been included in Appendix A.

2.3.1 Channel Mapping Scheme

One such selective scanning scheme is the Channel Mapping Scheme. The Channel Mapping Scheme aims to reduce the scanning time by using a selective scanning algorithm and caching mechanism. In the selective scanning algorithm, only a well-selected subset of all channels is scanned [6]. The principle uses the fact that all channels overlap except for channels 1, 6, and 11, and hence most APs are found in these channels.

The cache mechanism is used to further reduce the handoff delay. It does this by storing the handoff history of the mobile node. With each AP that the mobile node associates with, a cache entry of that AP is inserted into the cache. When the handoff is about to happen, the mobile node first checks its cache for the MAC address of the current AP. If there is a corresponding cache entry, the mobile node does not even scan but simply associates to the correspondent AP. Further details of the implementation of the Channel Mapping Scheme can be obtained from [25].

The problem with the Channel Mapping Scheme is that the mobile node only does full scanning once and after that, it does not have any means to update the information about the surrounding APs. That means that the Channel Mapping Scheme is at most a temporal solution for the next few handoffs if any.

Added to that, the Channel Mapping Scheme always scans at least three channels (i.e. the non-overlapping channels 1, 6, and 11) because it assumes that there should be APs in those channels, which is not always true. In addition, even though the cache is a useful enhancement to the Channel Mapping Scheme, it does not help with scanning but acts as a predictive mechanism for the next handoff. Furthermore, the caching is prone to errors because an entry indicating a handoff relationship between A1 and A2 does not mean that when a mobile node is handing off from A1 it will always be connected to A2.

University of Cape Town

2.3.2 Neighbour Graphs Algorithms

Another method that can be referred to as a selective scanning technique is that of the Neighbour Graphs (NG) Algorithms. NG Algorithms propose two link layer handoff schemes. These are the NG algorithm and the NG-pruning algorithm [5]. Both of these algorithms use the neighbour graph data structure. The NG-pruning algorithm further improves the scanning process by using the non-overlap graph data structure [5]. Both methods reduce the number of probed channels, and the time spent on each probed channel. The NG-pruning algorithm further reduces the number of probed APs. The Neighbour Graph stores information that depicts APs that have a handoff relationship. If AP 1 has a handoff relationship with AP 2, AP 2 is set in the neighbour graph as a neighbour of AP 1, and AP 1 becomes a neighbour of AP 2 [6].

In all the implementations of NG Algorithms however, the first edge handoff always experiences high latency. Also with growth of the graph, the AP list also grows meaning that one can end up scanning all the channels anyway. Another particular criticism of the proposed NG algorithms is that they do not take into account the direction of communication, and even though the algorithms perform much better than conventional methods, they are liable to cache misses. Added to that, if the mobile node uses the User-oriented method of implementing its table, it will have a slowly growing table according to the definition of how the table grows . On top of that, the Adaptive NG suggested in [5] is reactive rather than proactive which restricts the system from full effectiveness.

2.3.3 Discussion

The Neighbour Graph Algorithms necessitate the APs to do some work in updating the NG table when operating in the centralised or distributed method. The centralised method of implementing Neighbour Graphs is similar to the use of the Remote Authentication Dial-in User server (RADIUS) employed in IAPP [24]. IAPP is a protocol that outlines a standardised way for all APs to communicate, regardless of the vendors [14] that make them. The RADIUS server allows the IP addresses of neighbouring APs in an ESS to be looked up and based on their BSSID. That means that a node can dynamically get information about other APs from the NG-servers in Neighbour Graphs and from the RADIUS server in IAPP. In our system, the AP-Table server plays a similar role played by the RADIUS server in IAPP and the NG-Server in Neighbour Graph Algorithms. A mobile node in our system retrieves AP information such as position from the AP-Table server while connected to the current AP. This means that the retrieval or access to the AP-Table server is done before handoff occurs.

Another task performed by the mobile node is the retrieval of its own

University of Cape Town

position, which is done independently of the WLAN handoff. Using its own position and direction, the mobile node is able to calculate and determine the most suitable next AP (i.e. the AP that will give it the best wireless connection). In this way, the mobile node will know the AP which will give it the best connection before handoff rather than using the time consuming Full Scanning technique.

The accuracy and frequency of location updates is therefore vital to the success of operation of our system. The next section looks at the location issue and how location information can be used improve the link layer delay during handoff. We also explore available location update mechanisms.

2.4 Location Aided Handover

Location Aided Handover (LAH) utilises information about wireless network entities in the neighbourhood of a mobile node to aid in the handover process [28]. LAH decisions can be used to prevent the triggering of handoffs that result in short visits to discovered AP coverage areas.

LAH can also be used to effectively track the movement of a vehicle [19]. The desired destination of the vehicle is entered into a navigation system, which then calculates a route to the destination, along with the expected APs on the route. The movement of the vehicle is correlated to the calculated route as the vehicle moves and, in this way, a mobile node in the vehicle can make decisions on the next AP to use by reading the AP map along the route [19]. The problem with this scheme however, is that the mobile node has to stick to the predefined route otherwise the system fails. Added to that, the mobile user has the burden of entering route information for the destination all the time.

We present a location aided handover scheme that works at the link layer and does not require the mobile user to stick to a predefined route or to enter destinations in a navigation system. Our research uses LAH as a method to speed up the discovery of APs or improve latency at layer two during handover, which is something that has not been done before according to the reviewed literature [26].

2.5 Localization - Global Positioning System (GPS)

In LAH, a localization mechanism is usually used by the mobile node to obtain its position. Our proposed system, which is fully presented in chapter three, also relies on the mobile node using a localization technique for its position. The localization mechanism works independently of the WLAN handoff in our system. The requirement from a localization mechanism is that it gives position coordinates of the mobile node frequently and accurately.

University of Cape Town

Localization techniques can be classified into two categories: range-based and range-free techniques [38]. In range-based techniques, information such as distances or angles of a receiver are computed for a number of reference points using either signal strength, or timing based techniques and then the position of the receiver is computed by using some multilateration technique [39]. In range-free techniques, the receiver does not depend on the presence of any such information.

The localization mechanism considered here is GPS. Considering that APs have coverage of 100-150 meters outdoors and 30-50 meters indoors, it is imperative that the localization technique is suitable for the proposed systems. In this section, we give an overview of GPS as a way for a mobile node to have its position when moving outdoors. The discussion on indoor localization techniques can be found in the Appendix B.

In the Global Positioning System a mobile node can pin point its position through using satellite communication. GPS was first conceived after the launch of the first satellite called Sputnik 1 in 1957. Scientists realised that by measuring the frequency shifts in the small bleeps emanating from this satellite it was possible to locate a point on the earth's surface [2]. GPS became freely available to the public only after 199l when uses for GPS started escalating. The uses include frequency counting, Intelligent Vehicle Highway Systems (IVHS), Car Navigation Systems, Geographic Information System (GIS), Security, Aviation, Emergency Systems, census taking, forestry and many more. GPS is also starting to permeate the Laptop community [33] and there are many USB pluggable GPS receivers that are quite affordable and are as small as a flash memory stick [31, 32]. Hummer has recently released a laptop that comes equipped with a GPS receiver [3]. GPS does have its drawbacks however. For starters, its usage is dependant on the application, type, size, and access type allowed to the receiver. Access type could be Standard Positioning Service (SPS) or Precise Positioning Service (PPS). Added to that, a GPS receiver might have temporary outages as it passes under all kinds of obstructions that might block the satellite signal [27].

The reliability and accuracy of GPS has grown over the years. Nowadays, Vendors of GPS receivers are able to get reception accuracy for dynamic positioning of 20 mm (1"), 20 times per second with a latency of less than 20 milliseconds for example [30]. This means that a mobile node can have a record of its position every 50 ms. Therefore, a velocity update is actually possible every 50 ms.

2.5.1 GPS Operation

The Global Positioning System has three parts: the space segment, the user segment, and the control segment. The space segment is made up of satellites, the user segment consists of receiver devices that are held at the

University of Cape Town

user, and the control segment is made up of ground stations. The user segment consists of receivers, which you can hold in your hand, mount in a vehicle, aircraft, tanks or even submarines. These receivers are able to detect, decode, and process GPS satellite signals. The control segment consists of ground stations that make sure the satellites are working properly. The master control station is located at Schriever Air Force Base, in Colorado and other unstaffed monitor stations have been set up in different places in the world. In the space segment, there is a constellation of 24 satellites each in its own orbit above Earth.

Each satellite is equipped with an atomic clock that is accurate to within three nanoseconds. A signal is sent at frequencies of 1570-1580 MHz and it travels at the speed of light. This makes GPS ideal because its operating frequencies of 1570-1580 MHz are different from the 2.4 GHz operating frequency of 802.11b, meaning that a mobile nodes communication with APs will not be disturbed or interfered with in the presence of GPS signals. To find its position, GPS equipped node uses equation(1) below:

Equation(1): $Ds = (Tr - Ts)c$

The difference between the times when the signal is received (Tr) and when it was sent (Ts), multiplied by the speed of light (c), enables the receiver to calculate the distance (Ds) to the satellite [35]. To calculate its precise latitude, longitude, and altitude, the receiver measures the distance to at least three separate GPS satellites and then uses trigonometry or multilateration to find its position. The mobile node gets knowledge of other AP positions from the AP-Table server. Using its own position coordinates, the mobile node is then able to calculate distance to other APs.

The most accurate GPS receivers are those that use Differential GPS as an optimization to the position prediction. Differential GPS is a method of eliminating errors in a GPS receiver to make the output more accurate [2]. An addition to DGPS is real-time DGPS that does the process that DGPS does at real time for real time applications. Assisted GPS (A-GPS) was found to be the most accurate of all the standardised outdoor positioning methods by Motorola [26] improving the accuracy to 1 meter.

Other techniques for improving the precision of GPS include the Wide Area Augmentation System (WAAS), Local Area Augmentation System (LAAS), and Exploitation of DGPS for Guidance Enhancement (EDGE), Carrier-Phase Enhancement GPS (CPEGPS), Wide Area GPS Enhancement (WAGE), and Relative Kinematic Positioning (RKP).

University of Cape Town

Chapter 3

Integration and Usage of Location Information in Handoff

University of Cape Town

This chapter describes a proposed system for achieving fast 802.11b handovers by optimising link layer scanning. The entities which provide location information are presented and explained. An overview of how the system works is first given.

3.1 How the System Works

A mobile node has to have a localization technique in our scheme. It is imperative however that the method used for localization be kept independent and backward compatible with the normal methods of Full Scanning. That is because, if you only rely on an outdoor localization technique such as GPS, its uncertainty of availability due to obstacles, would sometimes lead to the mobile node not getting the necessary location information in good time to complete our algorithms. If it is backwards compatible to the conventional full scanning method, the system will still be able to operate and complete its handoff albeit consuming more time.

In real world systems, normally the location updates employed in the localization technique are based on the speed of the mobile node. If the mobile node is moving fast, the location update period is automatically made higher than when the mobile node is moving slowly. The indoor localization techniques covered in Appendix B are useful because they are very accurate. However, given the fact that an AP has more coverage in an outdoor area, our research will focus on the GPS system since it is suitable for outdoor environments. Figure 3.1 shows how GPS would work in our proposed system.

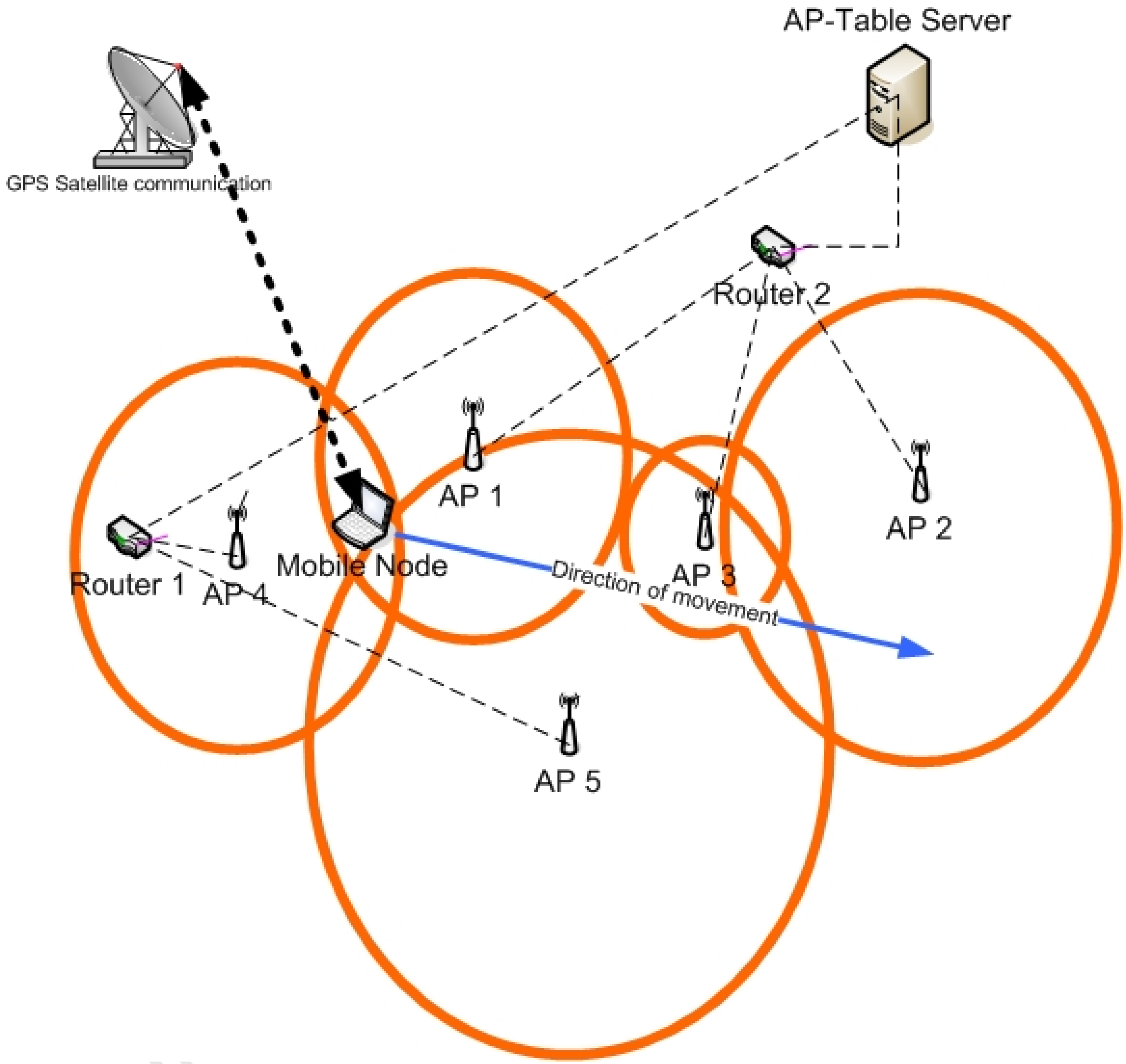


Figure 3.1: How GPS works in our proposed system

Real world configurations are not always similar to that of figure 3.1. They differ in topology, shape and size along with other network configurable characteristics. Added to that, there are normally a number of mobile nodes in motion instead of just one. Given the above network, the mobile node would use GPS communication to know its position. The mobile node would also receive information from the AP-Table server via its current AP about the geographic locations and RSSI ratings of other APs in the area along which it is moving in.

In order to determine the suitability of the next AP, a mobile node might look at a number of things in real world configurations including the Quality of Service (QoS), RSSI, etc. For this study, only the RSSI and positions of the APs, and the direction and position of the mobile node have been considered. QoS parameters such as the jitter, delay and bit rate that the mobile node will experience will not be considered or included in our simulations because the QoS required by a mobile node is determined by the application that requires connectivity. Our focus is more on on how fast a mobile node can connect to a new AP.

If the mobile node is connected to its current AP, and wants to handoff, it will use an algorithm to concatenate its GPS position with the AP-Table server entries to predict which AP is most suitable for its next handoff.

Using the RSSI rating of an AP plus how far the AP is from the mobile node, the actual RSSI that is experienced by the mobile node can be calculated using the RSSI-to-distance relationship formula or Free Space Path Loss formula. The next section will explain the Free Space Path Loss formula. Added to that, the direction of traversal of the mobile node is used to determine which AP will give it coverage for the most time before the next handoff. Taking figure 3.1 as an example, when the mobile node is connected to AP 4 in the diagram and wants to handoff, it would use its direction to determine that AP 5 would give it the longest coverage for its destination compared to AP 1 and AP 4.

There are two proposed algorithms used which will lessen the time to complete link layer handoff. These are namely the AP Response and Single Channel Scan algorithms. The latter lessens the time to that which is equivalent to scanning one channel, whereas the former further optimises the Single Channel Scan time by associating as soon as the desired probe response is received. These proposed algorithms will be compared with the currently employed Full Channel Scan method of 802.11b.

The mobile node cannot operate on its own in order to perform either of the proposed algorithms which lessen the link layer latency at handoff. Both of the proposed algorithms dictate that the mobile node only scan the channel where the most suitable next AP is expected. To do this, the mobile node must use information which it obtains from the AP-Table server while connected to its current AP.

The best case scenario for our algorithms is if the AP is found in the expected channel. If however, the mobile node does not find the expected AP in that channel, it would jump to the next channel where the next best AP is expected. To achieve this, the mobile node reorganises the AP information list that it gets from the AP-Table server in to a Scanning Sequence table. This reordering of tables is shown below in table 3.1.

University of Cape Town

Table 3.1: Reorganising from an AP-Table to a Scanning Sequence table

Table a) received from AP-Table server

Channel	AP	SNR Rating	Position
3	AP 1	10	12,181
9	AP 2	20	33,56
1	AP 3	56	46,944
8	AP 4	23	54,235
11	AP 5	29	788,879

Table b) showing rearranged table into a Scanning Sequence table

Channel To Scan	Expected AP	SNR Actual	Expected Time in AP coverage
11	AP 5	24	200s
1	AP 3	22	178s
8	AP 4	30	152s

University of Cape Town

To have this list in an orderly fashion, the mobile node uses the positions coordinates and RSSI ratings of the APs to calculate and determine (using the Free Space Path Loss formula) whether the actual RSSI that will be experienced by a mobile node at a certain position will be good enough to deliver sufficient service or coverage to it. If the mobile node does not determine a sufficient actual RSSI from an AP, the AP is not included in the Scanning Sequence table. After that, the mobile node then calculates which APs amongst the ones not discarded will give the mobile node the most coverage for the most time. To do this, the mobile node uses the direction that it is moving in [26].

The reason for considering the coverage time, is that there might be an AP which gives a higher actual RSSI, but when chosen would cover the mobile node for only a short time, forcing it to make another handoff. This for example can happen when a mobile node undergoes handoff to the next AP whilst moving away from it. Upon reaching its destination, the mobile node would have completed too many unnecessary and unintelligent handoffs. If in figure 3.1, the mobile node chooses to handoff to AP 1 instead of choosing AP 5, it will be forced to handoff to AP 3 or AP 5 before handoff to AP 2 occurs resulting in an extra handoff that could have been avoided had the mobile node had the intelligence to know that AP 5 is most suitable and will eliminate the need for another handoff.

The list for scanning can change from that received from the AP-Table server shown in table 3.1a) above to that of table 3.1b). AP 1 and AP 2 would be discarded by the mobile node as potential APs due to the Free Space Path Loss calculation deeming their actual RSSI to be inadequate from their positions in relation to the mobile nodes position. Once the Scanning

Sequence table has been created, the two proposed scanning algorithms can then be used effectively.

Figure 3.2 below shows diagrammatically how our algorithms improve the time taken in scanning at the link layer given that AP 10 in the figure operates in channel 11.

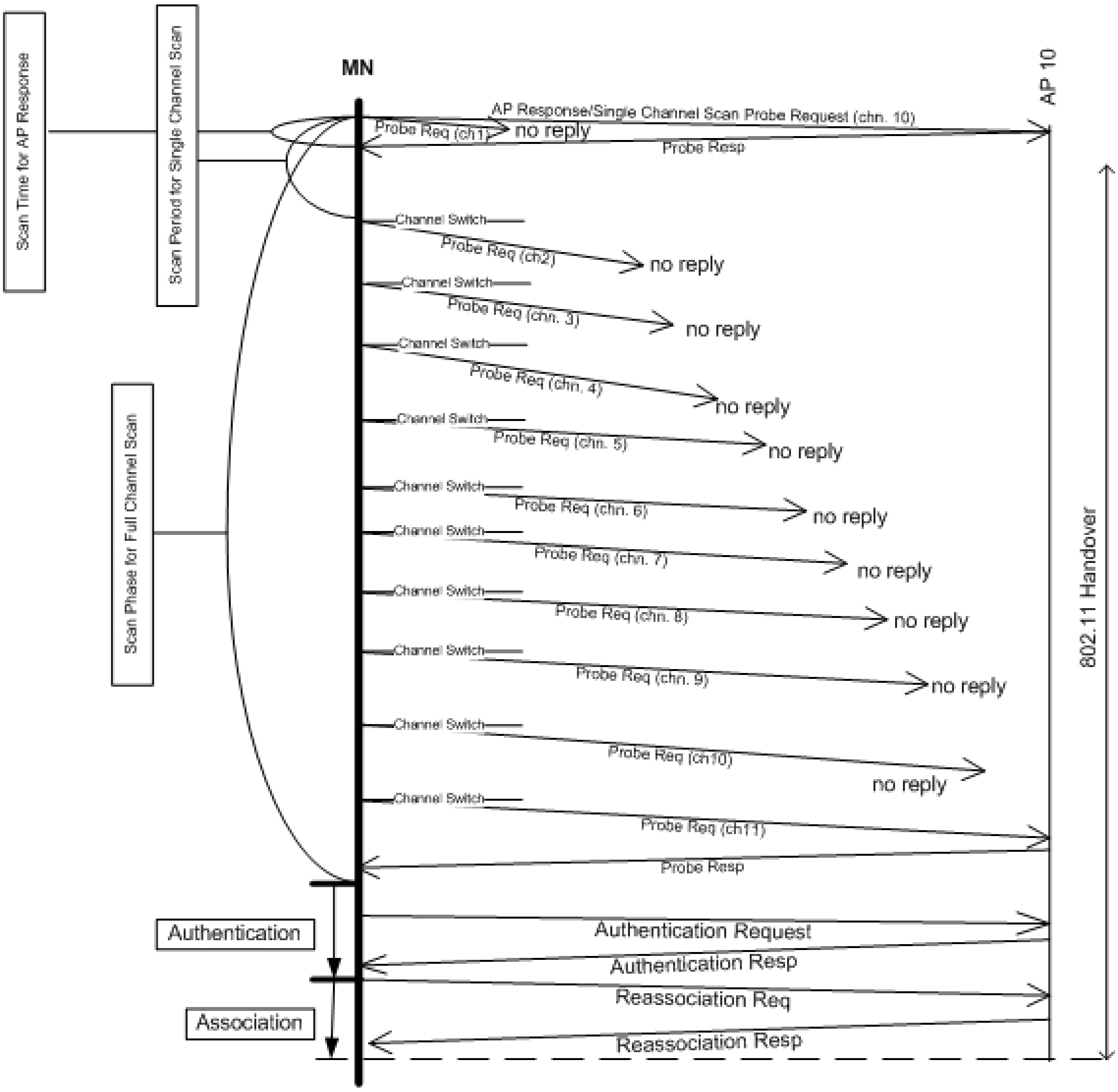


Figure 3.2: Comparing the Proposed Algorithms

Figure 3.2 shows that Single Channel Scan would be expected to perform better than Full Channel Scan, whilst the AP Response Scan method would be expected to perform even better than Single Channel Scan.

3.1.1 Single Channel Scan

Single Channel Scan is one of the solutions proposed. This algorithm lessens the time to that which is equivalent to scanning one channel. The sequence of what the mobile node does is shown in the flow chart of figure 3.3.

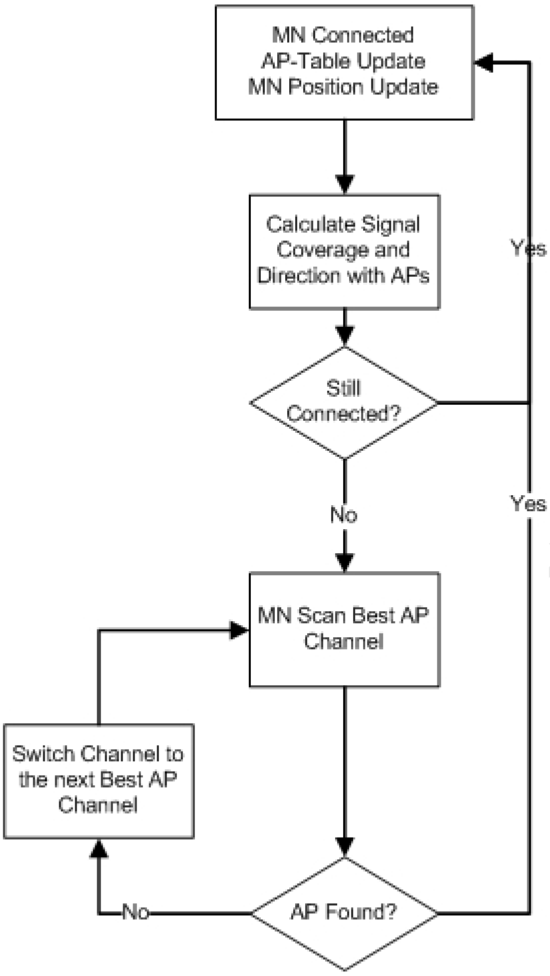


Figure 3.3: Single Channel Scan

Cape Town

In this technique, the mobile node only scans one channel. Using table 3.1b) as an example, the mobile node would start scanning from channel 11 looking for a response from AP 5. After *MaxChannelTime*, the mobile node would check whether it received the correct probe response and then continue to associate. Figure 3.2 shows that Single Channel Scanning will outperform the Full Channel Scanning method which always scans all available channels. The mathematical proof is that; if it takes x ms to scan one channel, then it will take 2*x ms to scan two channels. Meaning that with more channels scanned, the link layer latency increases proportionally. Therefore because

Full Channel Scanning scans more than one channel, it will always take longer than the time required to scan one channel.

Taking N to represent the total number of channels , Tb to be the *MinChannelTime*, Tt to be the *MaxChannelTime*, and t to be the total measured latency to find and associate to an AP, equation(2) below can be used to explain the time limits of the Single Channel Scanning method:

Equation(2): $N * Tb < t <= N * Tt$

In Single Channel Scanning, because the mobile node has a means of knowing its location and its next AP and which channel it operates in beforehand, N in equation(2) can be reduced to one.This would happen if the mobile node finds the next AP in the expected channel. This would then make t to be equal to Tt and hence, make the system more responsive and faster.

3.1.2 AP Response Scan

AP Response Scanning, makes the system even more responsive and efficient. This improvement is shown in the flow chart of figure 3.4. Here, the mobile node does not necessarily wait for the *MaxChannelTime* to elapse, but simply associates as soon as it gets the expected probe response. AP Response dictates that the mobile node stop scanning immediately after finding the respective AP that it is scanning for.

University of Cape Town

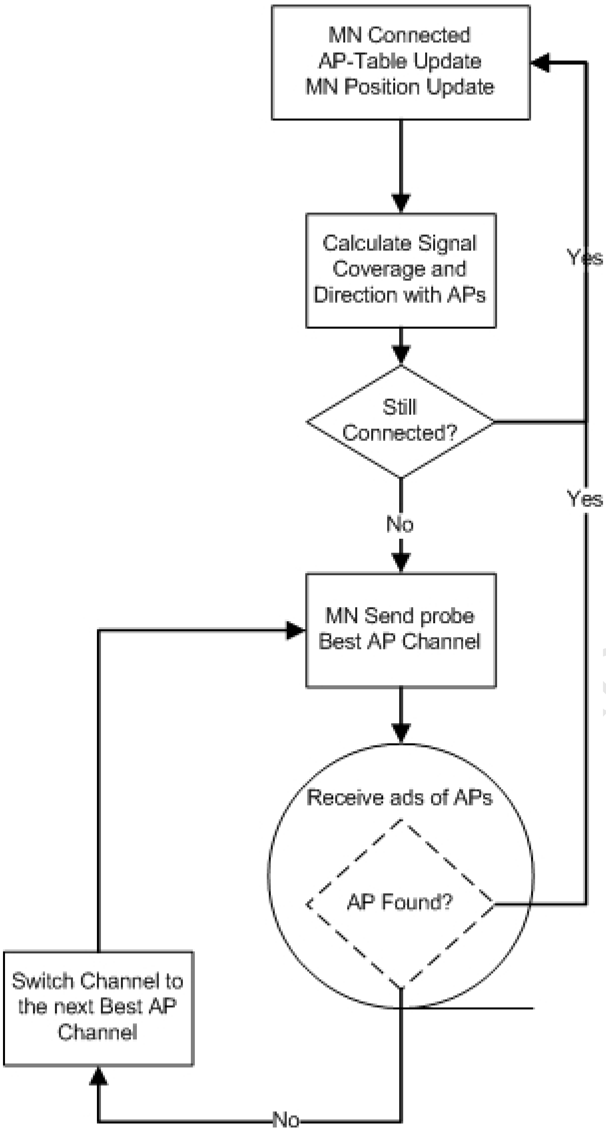


Figure 3.4: AP Response Scan

This means that the AP Response method will in most cases outperform Single Channel Scan, and because of that, it will also subsequently outperform the Full Channel Scanning method. In AP Response Scanning, the scanning time t from equation (2) above falls between zero seconds and Tt as shown in equation (3) below:

Equation(3): $0 < t < Tt$,

thus further shortening the time spent during scanning.

3.2 Entities of the Working System

Now that the way in which the system works has been presented, this section now gives the entities which realise the operation of the described system.

3.2.1 Localization Management System

The role of localization management in our system is to provide location information to mobile nodes. The mobile node integrates this information with layer two handover events in 802.11b to construct the Scanning Sequence table. Localization management can be achieved by a method such as GPS.

The GPS can be used to find out the coordinates of APs that populate the AP-Table server. This however would be done when the APs are set up for the first time because the APs would typically not move anywhere after installation. Hence the APs would not require a GPS receiver in them since it would only be used once. To find the coordinates of the APs, the installer would simply have a GPS receiver during installation and take the reading of the position of an AP installation point, and then later populate the AP-Table server with this information.

The mobile node can get position updates at predefined periods. A higher frequency of position updates gives a more accurate position of the mobile node over time. Ideally the position of the mobile node must be more frequently taken when the mobile node is moving fast and taken less frequently when it is moving slowly or is stationary.

University of Cape Town

3.2.2 Free Space Path Loss Formula

Free Space Path Loss (FSPL) is used to calculate the actual RSSI that would be experienced by a mobile node that is at a certain distance from an AP. This formula is shown below [12].

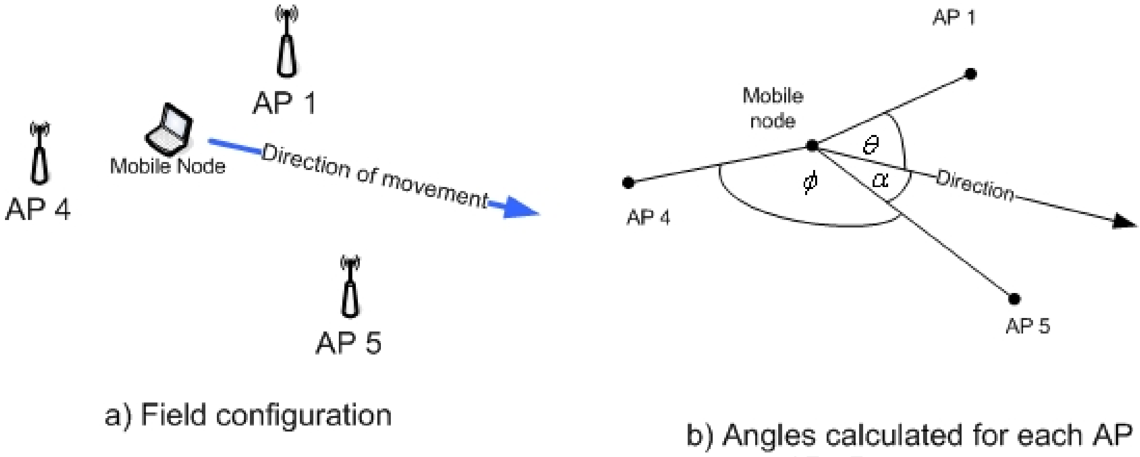
Equation(3): $\mathrm{FSPL} = 20 \cdot \log 10(d) + 20 \cdot \log 10(f) - 147.56$

Equation(4): $\mathrm{RSSI} = TS - \mathrm{FSPL}$

Where d is the distance between nodes in meters, f is the frequency of the signal in hertz and TS is the Transmission Signal or Transmission Rating of the AP. RSSI would be the SNR in dB that the mobile node would experience at distance d.

3.2.3 Calculating Direction to APs

Added to the calculation of the RSSI value explained in section 3.2.2 above, the mobile node also determines the angle that its traversal makes with the candidate APs that it could possibly handoff to. This is shown in figure 3.5.



a) Field configuration

b) Angles calculated for each AP

Figure 3.5: Calculation of Direction to APs

3.2.4 The AP-Table server

The AP-Table server acts as an entity that assists the mobile node to obtain the necessary information to make intelligent decisions. The AP-Table server is based on a relational database that looks like that shown in table 3.1a), and sits where it is reachable to the routers that connect the APs to the internet. The characteristics of the APs stored in the AP-Table server consists of the:

- AP: This is the Basic Service Set Identity of the AP. This would be the node identity of the AP.
- Channel: The channel that the AP transmits on.
- SNR: The signal to noise ratio of the AP or the power rating at which the AP transmits.
- Position: The position of the AP in terms of longitude, latitude and altitude.

These characteristics listed above are passed to the mobile node in the form of a message data packet at request. When entering a new AP coverage area, the mobile node would query the AP-Table server by giving its coordinates, and the AP-Table server would respond by sending a list of all APs within a certain range from the mobile node. Another function of the AP-Table server is to manage the addition and removal of APs. APs would need to be removed when they stop sending periodic announcements to the AP-Table server: a *lifetime* message. If an AP stops sending this message, it will be considered to have gone down and will be removed from the AP-Table server entries. The periodic interval for the lifetime message could be set to once every 24 hours. APs that go down for maintenance purposes will also send an

University of Cape Town

update message that will notify the AP-Table server when it goes down and when it comes up again. In our simulations however, the lifetime message along with removal of APs from the AP-Table was not implemented. An AP had an infinite lifetime in the system. Added to that, the kernel of our simulator was used to represent both the GPS that tracks the movement of the mobile nodes and was also used as the AP-Table server because it is able to track and record the positions of nodes in the simulation field. The mobile node simply had to query the kernel for the position of a node using that nodes identity and the kernel would reply with the position of that node.

3.2.5 The APs

The APs communicate with the AP-Table server to accomplish the followings tasks:

- Send lifetime update messages to the AP-Table server to announce their presence.
- Send messages to notify the AP-Table server whenever it goes down for maintenance.

3.3 Unimplemented Sections of the Architecture

Simulations were used to evaluate our system. Not all the sections of our proposed architecture were simulated. These parts which were not simulated are:

- The lifetime message along with removal of APs from the AP-Table was not implemented. An AP had an infinite lifetime in the system, and when mobile nodes missed an AP, they did not send an update to the AP-Table server.
- Obstacles that block the signals or the movement of the mobile node were not implemented.
- Our algorithms did not cater for when the mobile node does not find the expected AP in its channel. This is because obstacles were not implemented which perhaps could have blocked signals and created a situation where there would be AP misses. However, if an AP would not be found in its channel, the mobile node would look for the next best AP according to the Scanning Sequence table.
- Although data was simulated, our results do not include any references to data characteristics as the main concern was only on the latencies perceived at the link layer.

University of Cape Town

- Errors such as those of position inaccuracies were not implemented.
- The nodes in our simulations do not have an altitude field in the coordinates since we assume a two-dimension plane.

University of Cape Town

Chapter 4

Simulations of The Proposed System

University of Cape Town

4.1 Simulation Software

In our software simulations, better link layer handoff latencies were achieved by the mobile node during handoff. The simulation software used is called NCTUns 4.0 and is provided by Simreal technology [36]. NCTUns is a network simulator that is capable of simulating both wireless and wired networks [34]. This simulation software also has features such as the simulation of GPRS cellular networks, optical networks, wireless mesh networks, tactical and active ad hoc networks [36]. For our simulations, NCTUns version 4.0 proved to be easier to work with and provided the basic normal Full scanning algorithm. This algorithm was modified in certain parts to make it to adopt a Selective method of scanning. That is how we realised our goal of Full scanning versus Selective scanning. NCTUns also came with a kernel capability of tracking the simulation environment meaning that the mobile node and AP positions could be queried from the kernel thus simulating the tasks of the AP-Table server. The NCTUns kernel could also provide the direction of the moving mobile node via the math_fun.cc file which is found in the "\NCTUns-4.0\src\nctuns" folder of an installed NCTUns simulator. The file where parameters such as *MaxChannelTime* were configured, and where our selective method and direction algorithm was done was the mobilenode.cc file. These are available as resources of this thesis.

NCTUns was installed on a Fedora 7 linux platform. Two scenarios have been used to test the algorithms. The first simulation called Full versus Selective Scanning investigates how our architecture and algorithms are able to minimise the latency involved when finding the next AP. The second simulation is called Direction Aided handoff. This is where the total number of handoffs involved during a movement from one point to another in a maze of many APs is minimised through the implementation of our direction algorithm.

All our simulations in NCTUns 4.0;

- were run for about 4000s,
- the APs were set to have a coverage radius of 150 meters,
- the *MaxChannelTime* was set to 11 ms,
- the APs transmitted their beacons every 100 ms,
- the mobile node scanned actively, and travelled at a constant speed of 10 m/s which is equivalent to a car moving at 36 km/h.
- the kernel which represented the AP-Table server in our simulations, made location updates of the mobile node every second.

4.2 Simulations of Full versus Selective Channel Scanning algorithms.

Using simulations we simulated our two Selective Channel scanning algorithms and a third one which simulated the current original Full Channel scanning method. The topology used to evaluate Full versus Selective scanning is shown in figure 4.1. The exact coordinates of the APs is given in Appendix C. The RT 3 router is connected to AP 5 and gets data going to the mobile node via the RT 2 router. The RT 4 router connects to AP 6 and also gets its data from the RT 2 router. The Corresponding Node (CN) sends udp traffic to the mobile node via the RT 2 router. The mobile node moves back and forth along the shown traversal. When doing so it moves from the coverage of AP 5 and into the coverage of AP 6 and vice versa. Each of the three simulations averages about 100 handoffs. These simulations show that selective scanning takes a shorter time.

University of Cape Town

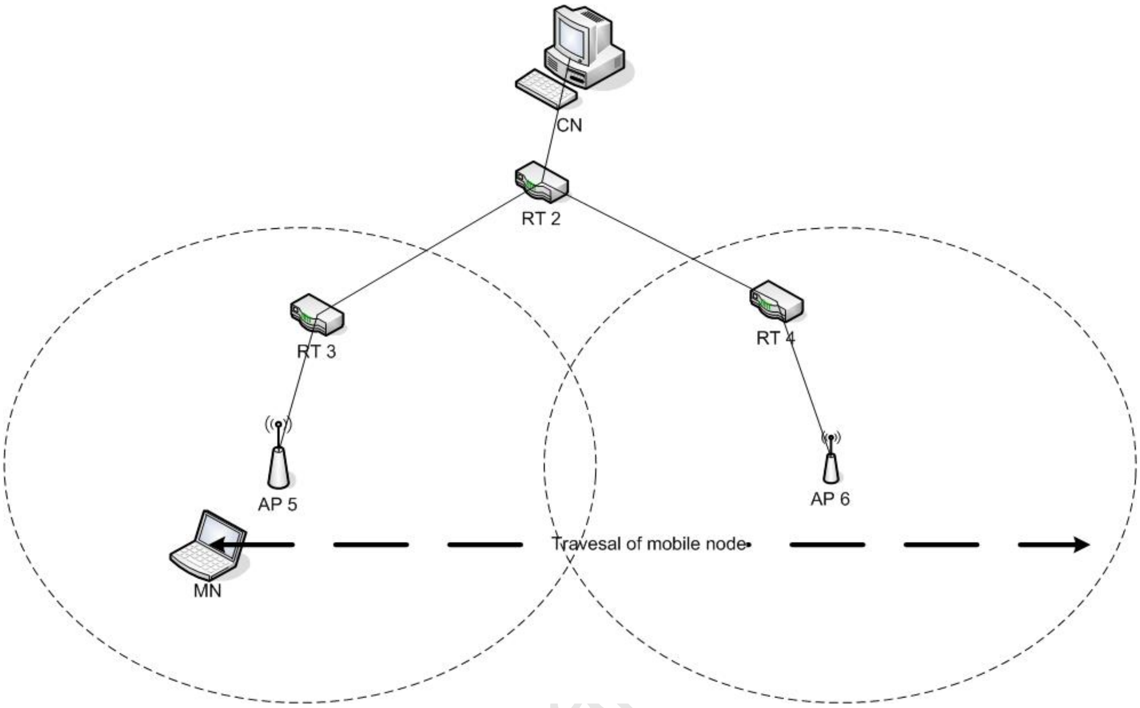


Figure 4.1: Simulation of Full versus Selective Scanning

University of Ca

4.3 Simulations of Using Direction to Minimise Frequent Handoffs

The simulation to minimise frequent handoffs was done between the Full Scanning method and the Single Channel Scanning method. The AP Response Scanning method was excluded here because its direction algorithm is identical to that of the Single Channel method, meaning that it would have similar results to the Single Channel method in terms of the total number of handoffs experienced by a mobile node after reaching its destination. The topology for these simulations included 22 APs scattered around the simulation environment. It is shown in figure 4.2. The exact coordinates of the APs is given in Appendix C. The traversal of the mobile node was not uniform but erratic for these simulations. Instead of only going back and forth, the mobile node could move to anywhere in the simulation environment and could move in all directions as shown by the arrows in figure 4.2. The same movement was implemented on both simulations and is given in Appendix D.

These simulations revealed that the Single Channel scanning method which has a direction algorithm experiences less handoffs at the end of the mobile nodes traversal.

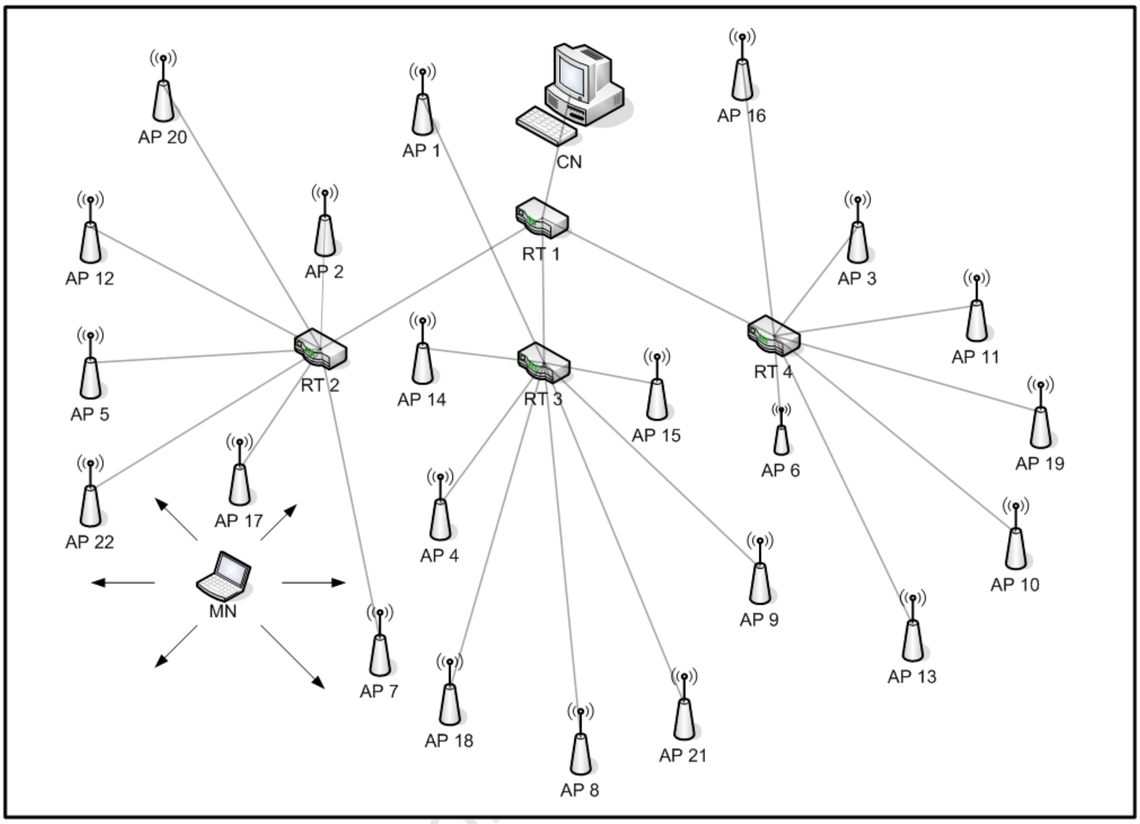


Figure 4.2: Simulation of Direction Aided Scanning

University of

Chapter 5

Results

5.1 Full versus Selective Scanning Results

In this scenario to model Full versus Selective scanning, the mobile node completes 101 handoffs per simulation. This simulation topology is shown in Appendix C and discussed in sectioin 4.2. The time for the beginning and end of link layer handoff were recorded to a file. The link layer latencies per handoff for the three schemes simulated are shown in figure 5.1. The averages of the latencies for each scanning algorithm is shown in figure 5.2. A table of the averages for each scanning algorithm is shown in table 5.1.

University of Cape Town

Table 5.1: Average Handoff Latency for each Scanning Method

Original Scan	Single Channel Scan	AP Response Scan
142.9882136 ms	11.00589216 ms	1.184705882 ms

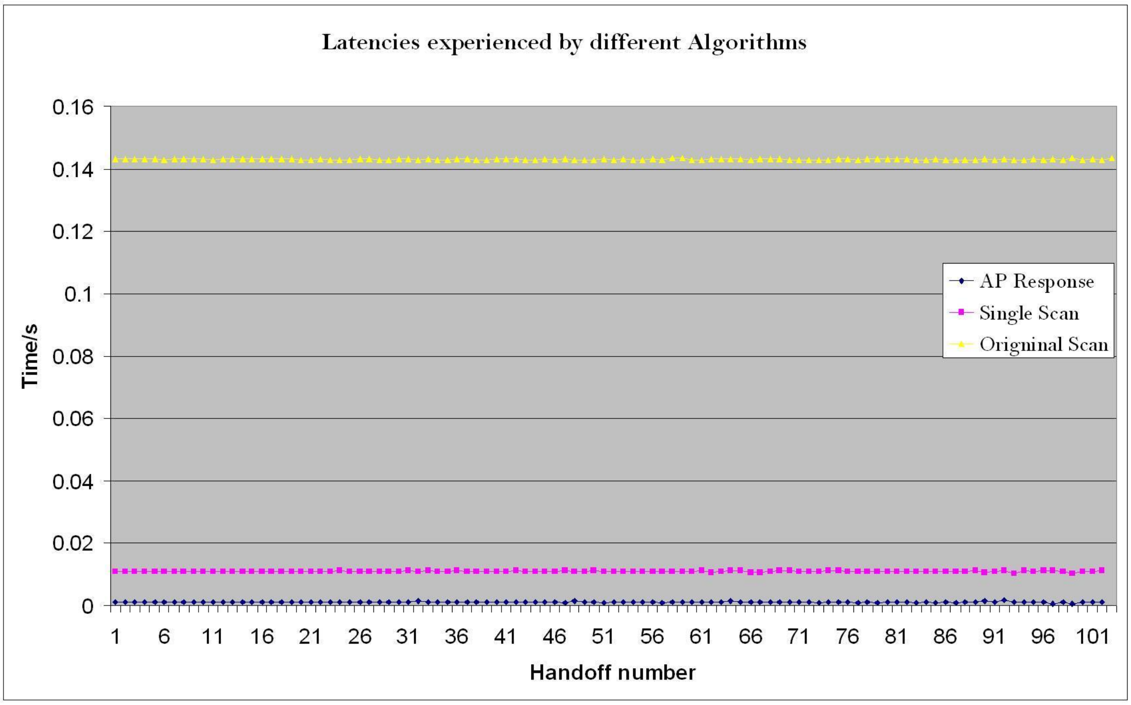
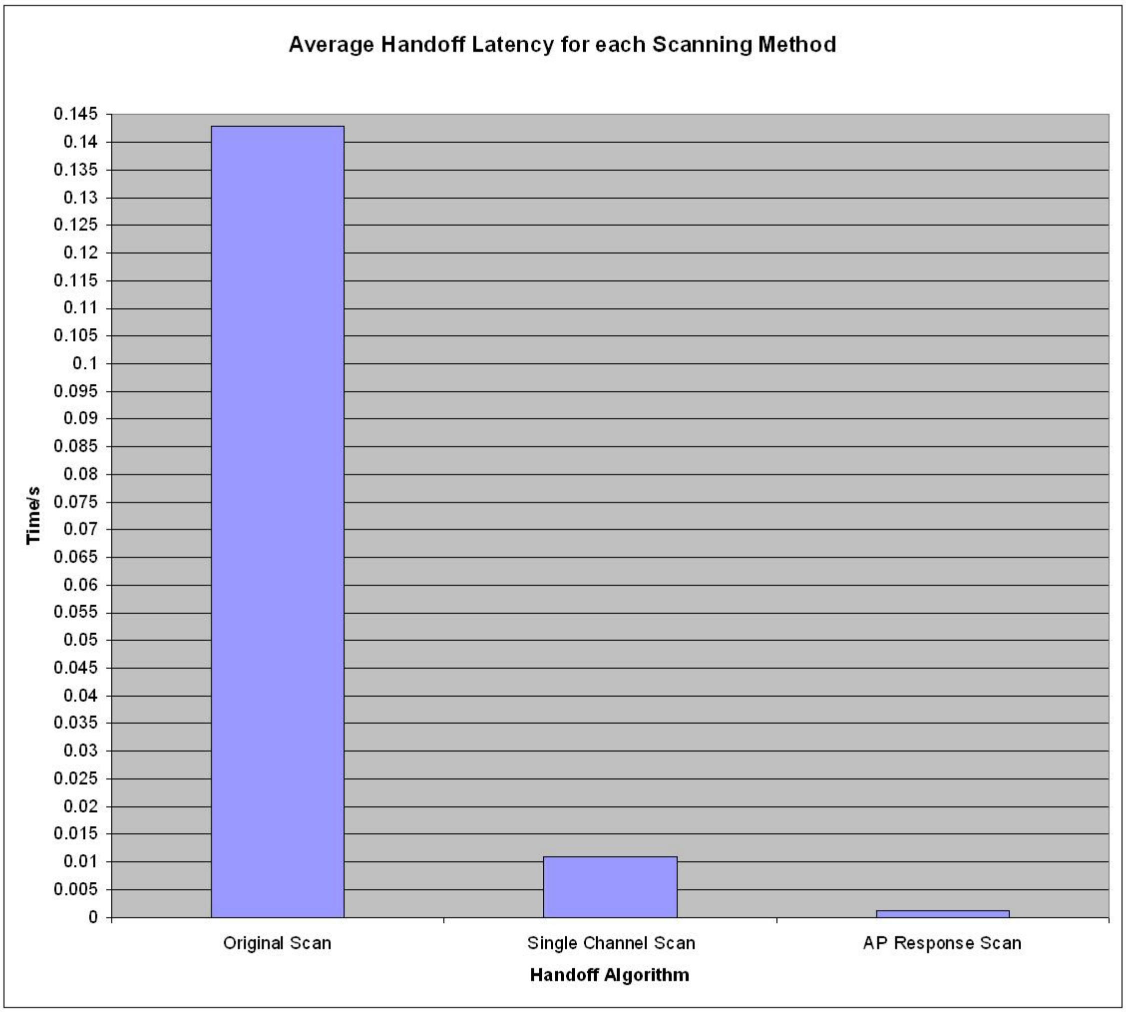


Figure 5.1: Latencies per Handoff for Simulated Algorithms

University



Unive

Figure 5.2: Average Latencies for Simulated Algorithms

The latencies of the different schemes show that the AP Response method is the best performer and the Full scanning method is the worst performer. In all our simulations, the Full scanning method has a latency that is proportional to the number of channels multiplied by the *MaxChannelTime* (ie 11 ms). The Full Scan method always uses about 143 ms for layer two handoffs. The Single Channel Scan method has a latency that is equal to the *MaxChannelTime*. Therefore, the average latency used by the Single Channel Scan method is 11 ms. The AP Response method has an average of 1.185 ms for link layer handoff latency. AP Response was therefore the fastest in executing layer two handovers.

5.1.1 Comparison of Proposed Scanning Algorithms with other Research

The relevant research looked at in chapter 2 includes NG, NG-pruning, MultiScan, SyncScan, and Channel Mapping. The handoff strategies that allow the mobile node to know which AP to attach to before handoff, have the lowest link layer handoff latency. Multiscan for example uses two wireless cards [9]. Its strategy of finding the available APs with a secondary card before handoff occurs helps to bring the link layer latency down to zero seconds. The NG and NG-pruning algorithms also has low latencies of around 20 and 15 ms respectively [5]. What is noticeable about the NG algorithms is that their latency time increases with increasing number of available APs. This means that the bigger the pool of neighbouring APs, the bigger the latency time incurred. Except for Channel Mapping and Multiscan, all of the other handoff techniques require some infrastructure modification [25]. The SyncScan algorithm also presents a maintenance problem because APs are required to transmit their beacons at the same time if they are in the same channel [22]. Over time, the timing of APs' beacon transmission will drift away from each other and the mobile node might not get all responses when it listens in a channel.

5.2 Direction Aided Scanning Results

The second simulations performed were those of adding a direction algorithm to our architecture to lessen frequent handoffs. In doing so, the mobile node created a MN-AP table before every handoff which calculated the best AP to be chosen. This was compared with the Full scanning method which chooses the signal with the strongest SNR received for its next AP coverage. During simulation, the MN-AP Table created by the mobile node was recorded. Along with the time for the beginning and end of the scanning phase, the parameters also recorded for Direction Aided scanning were those that were calculated by the MN when it eliminated unsuitable entries from the AP table. The identity of the AP chosen as the best AP chosen after scanning was also recorded in this scenario. The scenario is shown in Appendix C.

Table 5.2 shows the MN-AP Table which was created along with the AP which was chosen at that handoff.

University of Cape Town

Table 5.2: Direction Algorithm Calculations and the APs Chosen by the Mobile Node

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
1	18	21.569	3	-83.22011	18
	12	65.921	3	-74.24328	
2	15	33.872	3	-83.53743	15
	16	36.686	3	-70.89275	
	7	148.682	4	-73.37474	
3	8	109.582	3	-66.63195	8
	19	144.704	3	-85.42777	
4	23	6.366	3	-78.85734	23
5	8	44.219	3	-83.25466	8
	22	89.268	3	-83.28208	
6	15	34.983	3	-65.67038	15
7	18	45.766	3	-83.60287	18
	13	79.85	7	-76.95483	
8	28	4.567	3	-72.17294	28
	12	110.366	3	-78.43951	
9	13	29.717	7	-82.29239	13
	18	81.969	3	-81.55869	
	11	83.433	3	-80.94003	
	12	125.102	3	-83.37398	
10	15	71.284	3	-72.22875	15
	21	80.477	3	-83.54465	
11	22	35.765	3	-82.01459	22
	8	93.935	3	-84.89308	
	27	101.978	3	-78.21431	
12	8	3.618	3	-82.31495	8
13	24	42.286	3	-79.53389	24
	16	75.919	3	-77.98815	
	19	170.007	3	-67.02422	
14	25	12.35	3	-76.12131	25
	10	84.064	3	-74.51089	
15	6	95.066	6	-81.9718	6
	10	121.772	3	-77.91479	
16	12	23.437	3	-76.31052	12
	18	72.958	3	-81.96878	
17	20	1.94	3	-76.97322	20
	28	166.961	3	-68.37059	
18	11	19.905	3	-73.87914	11
	28	145.871	3	-85.07164	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
19	21	7.978	3	-78.50783	21
	13	153.361	7	-75.45321	
20	15	44.548	3	-73.8193	15
	13	140.497	7	-83.13211	
21	24	9.311	3	-82.43634	24
	19	77.8	3	-71.83535	
	7	113.141	4	-84.30043	
	16	151.756	3	-71.70987	
22		18.324	4	-72.36508	7
	10	38.135	3	-85.34519	
	16	133.018	3	-71.87982	
	19	177.873	3	-84.08794	
23	8	13.322	3	-85.04742	8
	19	40.318	3	-69.7554	
	15	88.248	3	-82.96255	
	16	161.678	3	-72.24954	
24	26	52.714	3	-77.48153	23
	17	126.524	3	-83.84486	
25	8	50.809	3	-79.98529	8
26	15	63.523	3	-74.24226	15
	27	98.612	3	-82.94738	
27	18	0.082	3	-81.6247	18
	7	57.286	4	-84.1223	
	13	119.63	7	-80.69064	
28	11	55.479	3	-83.90931	11
	28	91.943	3	-76.72775	
	12	166.559	3	-81.71995	
29	18	36.709	3	-74.31089	18
	12	92.858	3	-80.27238	
	13	96.39	7	-84.42952	
30	16	74.403	3	-74.09163	16
	10	85.511	3	-83.55657	
	7	153.739	4	-67.16243	
31	18	39.863	3	-82.72199	18
	10	98.485	3	-73.12163	
	7	112.868	4	-72.46355	
32	14	31.234	2	-81.23625	14
	28	55.342	3	-82.68134	
	12	131.477	3	-73.53116	
33	18	1.142	3	-81.25195	18
	12	31.53	3	-65.78817	
	28	117.862	3	-82.85513	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
34	15	29.975	3	-79.92402	15
	16	58.288	3	-73.17005	
	7	131.656	4	-78.00056	
35	24	29.727	3	-85.29032	24
	19	59.739	3	-59.67647	
	16	112.529	3	-80.62038	
	8	119.451	3	-80.13512	
36	7	16.979	4	-71.21851	7
	10	74.505	3	-85.036	
	16	106.835	3	-72.19018	
	19	146.102	3	-84.90628	
37	12	56.506	3	-74.51191	12
	18	152.916	3	-68.84699	
38	14	68.143	2	-73.60302	14
	28	135.704	3	-78.48398	
39	12	59.25	3	-74.55378	12
	28	109.201	3	-70.67929	
40	13	26.919	7	-77.48658	13
	11	86.21	3	-81.70507	
	18	117.567	3	-81.26708	
41	27	3.397	3	-84.27722	27
	21	69.227	3	-73.08075	
	15	105.194	3	-82.03678	
42	22	116.594	3	-77.50921	22
43	23	22.66	3	-76.12622	23
44	8	29.398	3	-79.14869	8
45	7	37.801	4	-84.33784	7
	16	61.189	3	-69.34071	
	19	116.933	3	-72.28179	
	15	134.557	3	-83.27288	
46	25	111.995	3	-82.87486	25
	10	174.094	3	-70.08473	
47	6	29.993	6	-80.52965	6
	10	177.231	3	-78.73292	
48	10	44.274	3	-70.48917	10
	25	56.639	3	-79.29559	
49	24	41.264	3	-73.80096	24
50	17	40.731	3	-76.38468	17
	8	50.975	3	-83.65636	
	19	108.884	3	-81.78839	
51	23	46.497	3	-78.56929	23
	26	165.648	3	-74.09179	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
52	22	58.606	3	-73.10505	22
53	15	3.152	3	-81.25778	15
	8	76.512	3	-84.70931	
	27	134.289	3	-79.57656	
54	13	29.815	7	-73.9075	13
55	11	152.649	3	-71.20789	11
56	28	48.952	3	-75.01553	28
	20	58.551	3	-74.48922	
57	18	59.263	3	-74.46611	18
	12	169.49	3	-65.98546	
58	16	29.649	3	-84.69291	16
	7	68.389	4	-72.60958	
	10	136.85	3	-72.75473	
59	17	24.199	3	-84.60253	17
	8	59.038	3	-78.30015	
	19	158.876	3	-72.12971	
60	8	119.514	3	-67.63574	8
61	22	30.649	3	-75.26525	22
	27	46.139	3	-80.27017	
62	21	2.141	3	-79.10613	21
	27	130.329	3	-69.47138	
63	11	17.562	3	-79.91916	11
	13	85.505	7	-74.94523	
64	12	2.921	3	-74.66004	12
	18	49.506	3	-81.25825	
	28	90.847	3	-79.37369	
65	10	18.35	3	-80.31877	10
	6	137.506	6	-83.00983	
66	19	31.908	3	-81.11915	19
	24	50.735	3	-75.92213	
	16	89.534	3	-78.36372	
	7	142.163	4	-82.22269	
67	15	86.135	3	-82.02761	15
	7	93.434	4	-74.74596	
	16	168.415	3	-70.70913	
68	13	31.336	7	-81.52343	13
	18	83.951	3	-81.62264	
	7	142.759	4	-83.43946	
69	15	84.067	3	-76.19468	15
	21	88.222	3	-78.9123	
70	19	72.275	3	-77.77118	19
	8	116.07	3	-65.65345	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
71	7	65.775	4	-74.39212	7
	15	113.836	3	-82.37097	
	16	166.593	3	-70.78211	
72	12	49.497	3	-79.70679	12
	18	109.998	3	-71.13017	
73	20	34.81	3	-78.56168	20
	28	107.866	3	-67.35484	
74	11	27.109	3	-73.33743	11
75	21	13.726	3	-79.51468	21
	13	123.963	7	-80.95752	
76	15	72.991	3	-82.4563	15
	27	148.24	3	-76.97665	
77	8	11.35	3	-60.76472	8
	19	64.5	3	-83.49271	
78	17	92.409	3	-69.9364	17
79	23	38.155	3	-81.50044	23
	26	151.424	3	-67.08572	
80	22	26.845	3	-73.11894	22
81	8	7.66	3	-77.61313	8
82	24	6.52	3	-76.6777	24
	19	129.434	3	-72.61121	
83	7	22.187	4	-72.59516	7
	16	76.761	3	-82.23086	
	10	94.8	3	-75.23719	
84	13	63.665	7	-85.21413	13
	12	89.567	3	-80.20017	
	18	147.331	3	-72.19911	
85	11	88.026	3	-73.75376	11
	28	100.737	3	-85.0855	
86	28	28.088	3	-72.7624	28
	12	32.341	3	-85.42938	
	20	114.35	3	-81.18112	
87	14	87.89	2	-75.16876	14
	12	137.688	3	-81.43721	
88	12	12.079	3	-67.11669	12
	18	47.072	3	-81.51597	
	28	64.896	3	-83.49029	
89	13	31.029	7	-78.68041	13
	11	37.711	3	-76.77702	
	18	142.126	3	-84.57648	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
90	16	4.714	3	-78.83301	16
	7	56.036	4	-78.22174	
	15	69.658	3	-82.96025	
	18	118.38	3	-83.66501	
91	24	88.059	3	-71.93949	24
	19	138.888	3	-76.35126	
92	15	15.73	3	-84.44566	15
	8	66.587	3	-80.47528	
	16	76.294	3	-78.36435	
	19	174.965	3	-63.5033	
93	18	20.739	3	-79.36494	18
	7	50.623	4	-79.89533	
	16	97.662	3	-83.96445	
	13	128.338	7	-84.73918	
94	11	37.28	3	-75.44023	11
	13	60.048	7	-71.95467	
95	21	17.846	3	-78.96224	21
	13	137.03	7	-75.3151	
96	22	0.485	3	-78.54992	22
	27	153.976	3	-64.09769	
97	15	5.338	3	-83.70686	21
	21	79.736	3	-84.97803	
	27	147.314	3	-73.93228	
98	7	39.231	4	-71.45037	7
	18	42.941	3	-81.55707	
	16	123.086	3	-76.83465	
99	13	22.321	7	-80.87927	13
	12	120.611	3	-85.473	
	18	156.032	3	-76.07741	
100	11	164.407	3	-72.37437	11
101	28	27.051	3	-72.61104	28
	20	73.158	3	-78.89635	
102	18	61.469	3	-73.87081	18
	12	131.011	3	-76.39627	
103	15	15.63	3	-79.26652	15
	16	56.339	3	-80.19106	
	7	106.136	4	-82.73249	
	13	121.942	7	-85.27765	
104	19	86.516	3	-68.42651	19
	8	111.69	3	-75.93519	
	16	120.291	3	-83.75178	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
105	17	106.132	3	-82.45238	17
	24	113.546	3	-84.13328	
106	8	112.927	3	-63.92591	8
	19	129.781	3	-85.12685	
107	22	38.856	3	-75.97694	22
	27	42.566	3	-78.55011	
108	21	74.638	3	-80.78398	21
	27	178.852	3	-70.57867	
109	15	77.123	3	-68.16912	15
110	18	40.674	3	-80.73423	18
	7	41.77	4	-73.17071	
	16	112.764	3	-78.59576	
111	11	25.402	3	-74.59215	11
	13	83.312	7	-82.68787	
112	18	30.563	3	-74.30603	18
	12	78.871	3	-82.33753	
	13	121.643	7	-83.05293	
113	10	68.716	3	-73.82955	10
	16	103.961	3	-83.51413	
	7	149.646	4	-71.99441	
114	16	16.96	3	-80.04213	16
	19	35.378	3	-82.53491	
	7	67.303	4	-82.5496	
	24	113.336	3	-75.17328	
115	15	138.609	3	-68.52055	15
116	27	49.222	3	-70.08487	27
	21	82.704	3	-78.32909	
117	15	56.946	3	-77.96347	15
	21	139.544	3	-77.52964	
118	18	22.564	3	-78.71918	18
	7	52.655	4	-78.97795	
	16	100.826	3	-83.70408	
	13	128.484	7	-85.40271	
119	6	11.794	6	-80.53069	6
	10	120.52	3	-84.63142	
	12	131.795	3	-84.68815	
120	12	19.316	3	-76.41028	12
	14	94.588	2	-83.22552	
121	11	31.971	3	-77.85435	11
	28	137.798	3	-82.04261	
122	13	171.716	7	-71.58009	13

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
123	16	38.697	3	-80.71118	16
	15	47.373	3	-72.58994	
124	17	25.373	3	-85.08928	17
	8	107.125	3	-77.92162	
	19	147.509	3	-71.56578	
125	16	4.459	3	-85.31942	16
	19	10.704	3	-69.67902	
	24	83.542	3	-82.29883	
	8	89.687	3	-82.32476	
126	13	63.218	7	-83.11144	13
	18	69.793	3	-76.42054	
	7	138.339	4	-82.47053	
127	28	52.036	3	-82.72004	28
	11	86.756	3	-79.40906	
	12	110.667	3	-84.00064	
128	20	120.513	3	-66.37487	20
129	14	5.015	2	-79.91675	14
	28	117.551	3	-75.07806	
130	6	90.809	6	-76.01062	6
131	10	19.642	3	-73.10122	10
	7	38.49	4	-85.18729	
132	24	37.99	3	-73.28903	24
	19	44.102	3	-82.60898	
	16	94.242	3	-81.75403	
	7	139.236	4	-84.35413	
133	17	29.233	3	-75.75092	17
134	23	68.744	3	-80.92952	23
	26	151.366	3	-81.00358	
135	22	24.267	3	-72.55533	22
136	8	52.345	3	-77.74987	8
	27	115.081	3	-85.1003	
137	16	11.305	3	-68.62616	16
	7	19.128	4	-84.47513	
	19	102.995	3	-75.00216	
	15	132.343	3	-78.62524	
138	10	13.491	3	-69.58553	10
	7	145.787	4	-75.09443	
139	18	18.297	3	-68.32448	18
	12	69.695	3	-75.92053	
	7	96.984	4	-82.541	
140	11	27.178	3	-73.65804	11
	13	67.481	7	-74.1243	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
141	13	178.02	7	-72.24121	13
142	16	22.015	3	-78.47853	16
	7	37.771	4	-79.07983	
	15	90.5	3	-81.97007	
	18	96.421	3	-84.54459	
143	24	67.124	3	-67.62706	24
	19	128.222	3	-85.45475	
144	15	6.249	3	-82.65296	15
	16	83.965	3	-70.5626	
	7	100.973	4	-85.35132	
	19	113.099	3	-71.47429	
145	21	51.122	3	-70.94272	21
	27	79.024	3	-77.71369	
146	15	70.976	3	-79.28458	15
	27	141.153	3	-79.72049	
147	19	69.958	3	-78.91154	19
	8	112.781	3	-63.32431	
148	17	101.952	3	-73.98007	17
149	8	113.351	3	-75.18976	8
150	22	2.845	3	-75.15047	22
	27	52.301	3	-85.42312	
151	8	69.818	3	-83.30502	8
	23	88.558	3	-84.16967	
152	17	42.442	3	-72.37295	17
	26	84.932	3	-77.77549	
153	23	44.458	3	-78.49327	23
	26	142.598	3	-78.75042	
154	22	95.444	3	-80.009	22
155	23	3.836	3	-76.42372	23
156	26	111.261	3	-75.78362	26
157	8	32.483	3	-77.82446	8
	17	118.894	3	-84.10446	
158	15	73.729	3	-71.74707	15
	27	95.655	3	-85.15993	
159	13	36.311	7	-73.62999	13
	21	113.597	3	-81.08581	
160	11	134.188	3	-73.13756	11
161	12	33.498	3	-82.38078	12
	28	45.944	3	-72.78801	
	20	112.076	3	-84.54136	
162	6	41.127	6	-82.23109	6
	14	117.811	2	-77.78255	

University of Cape Town

Handoff No.	AP ID	Angle	channel	expected SNR/dB	AP Chosen
163	25	43.351	3	-70.63901	25
	10	63.945	3	-78.37252	
164	18	10.739	3	-84.66951	18
	7	69.456	4	-78.42495	
	10	170.326	3	-68.76552	
165	11	63.663	3	-82.4449	11
	28	86.396	3	-78.53138	
	12	154.428	3	-82.82483	
166	20	104.856	3	-78.2098	20
167	14	29.685	2	-80.79908	14
	28	129.518	3	-79.31979	

Careful scrutiny of this table shows that the mobile node does not always choose the AP which will give it the strongest signal, but it rather chooses the one which makes the least angle with its own traversal. This is because if a mobile nodes traversal makes an angle of zero with the direction to the mobile node, the mobile node will pass through the middle of the AP meaning that the mobile node will pass through that APs coverage centre and hence get the most coverage. Taking the third handoff from table 5.2 for example, one can see that although AP 19 gives a stronger SNR which is -85.427770 dB compared to AP 8's SNR which is -66.631950 dB, the mobile node chooses AP 8 because the angle its traversal makes with the direction to the AP 8 is much smaller than that which is made by the direction to AP 19. Other handoffs where the mobile node does not choose the AP with the strongest SNR but the one where it is guaranteed the most coverage are handoff; 8, 9, 10, 11, 16, 18, 20, 21, 22, 24, 26, 27, 29, 30, 32, 33, 36, 38, 40, 48, 50, 53, 61, 64, 65, 66, 68, 69, 71, 75, 77, 83, 85, 86, 87, 88, 89, 90, 91, 93, 97, 98, 99, 101,102, 103, 104, 105, 106, 107, 111, 112, 113, 114, 116, 118, 119, 120, 121, 127, 131, 132, 134, 136, 137, 138, 139, 140, 142, 143, 144, 145, 146, 150, 151, 152, 153, 157, 158, 159, 161, 163, 165. This gives a total of 83 handoffs where an AP that was not the strongest was chosen.

The graph of figure 5.3, shows the total number of handoffs that our Direction Aided algorithm makes compared with the Full scanning method when the mobile node finally reaches its destination.

University of Cape Town

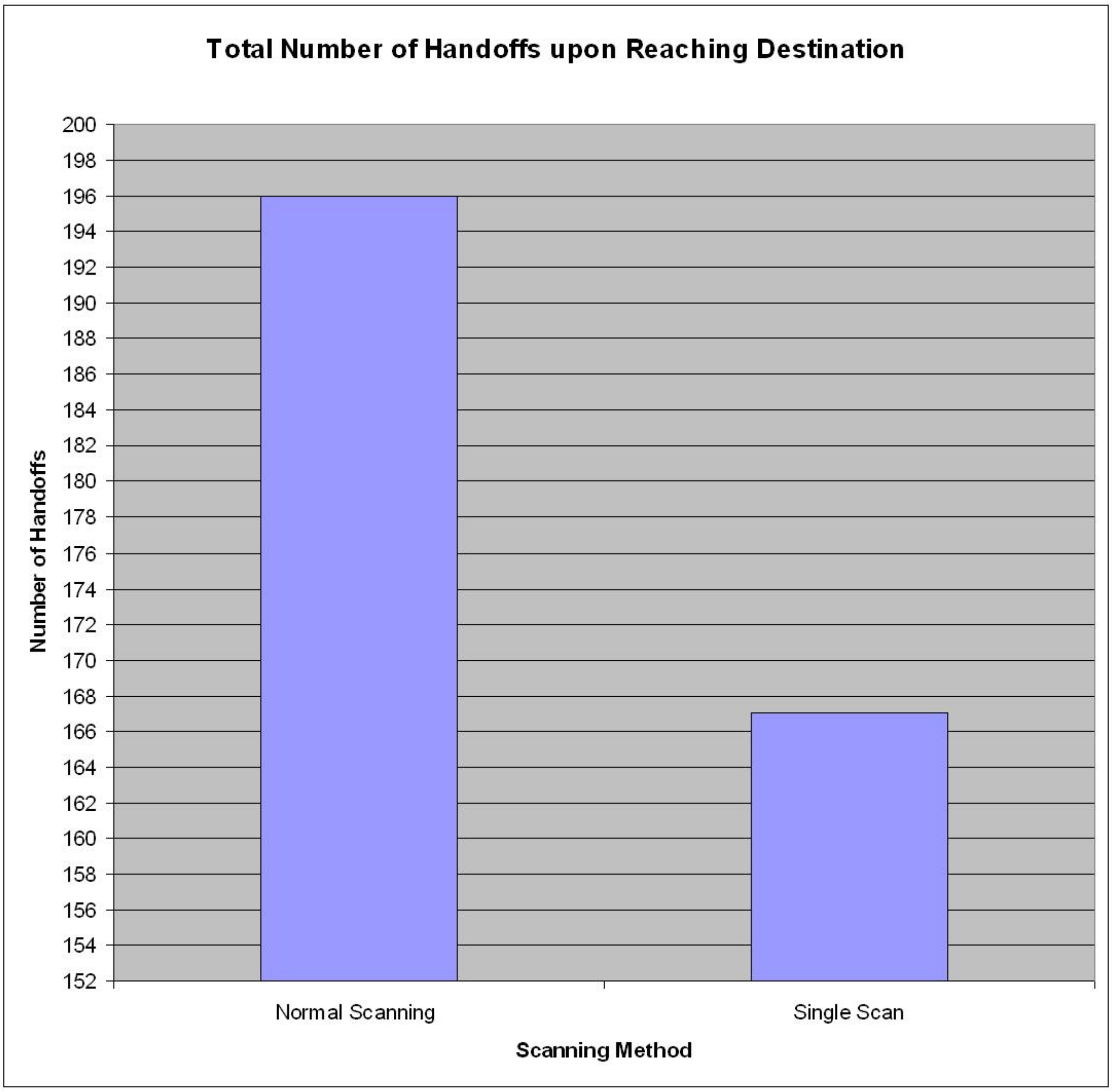


Figure 5.3: Total Number of Handoffs when Mobile Node Reaches its Destination

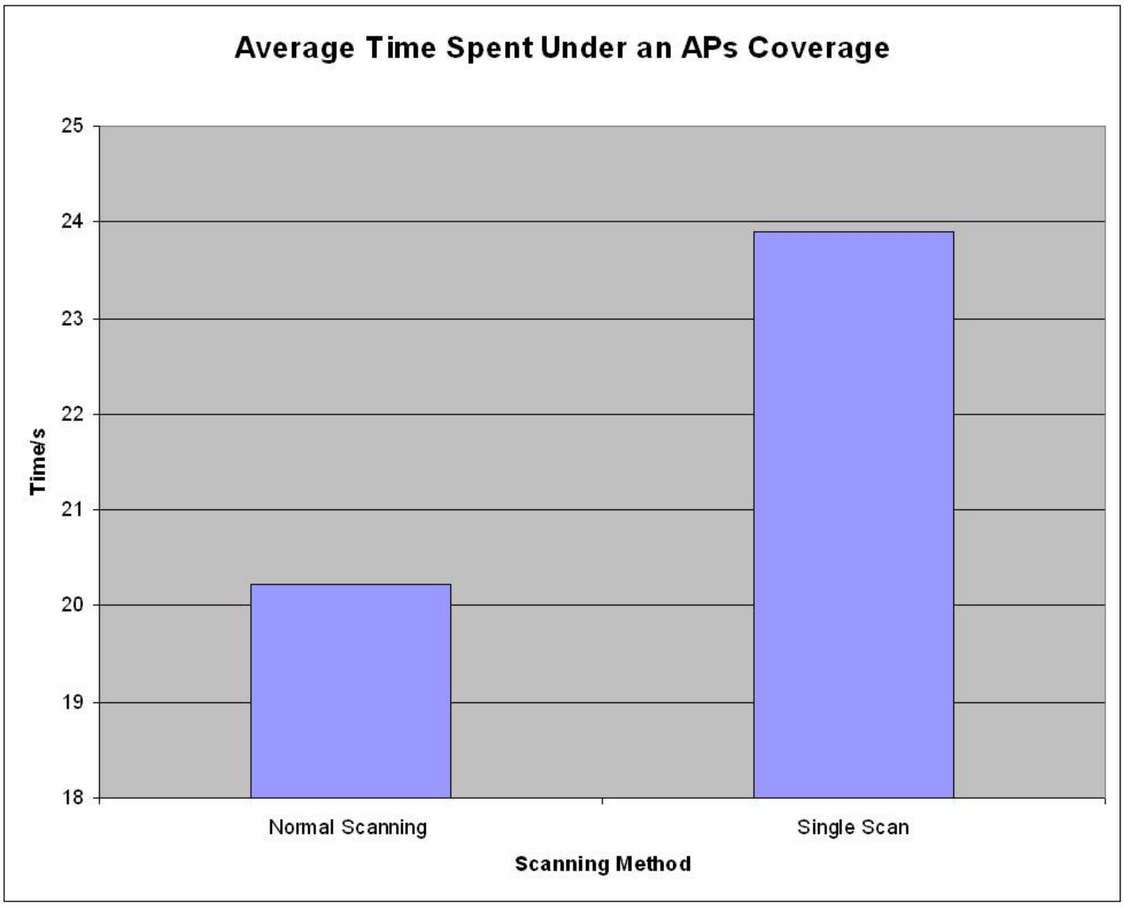


Figure 5.4: Average Time under an APs Coverage

Figure 5.4 gives an average of time spent under an APs coverage for the two implementations. This figure shows that with the Direction Aided algorithm, the mobile node spends more time on average under an APs coverage. This is also reflected by figure 5.5 which gives the area of time for the mobile node to complete its traversal. The area under the Direction Aided is similar to that of the area under the Normal scanning method which chooses the strongest SNR for its next coverage. In some instances, the mobile node is able to have coverage for above 70 seconds for Direction Aided handoffs, whereas with Normal scanning, the highest peak in time is under 40 seconds.

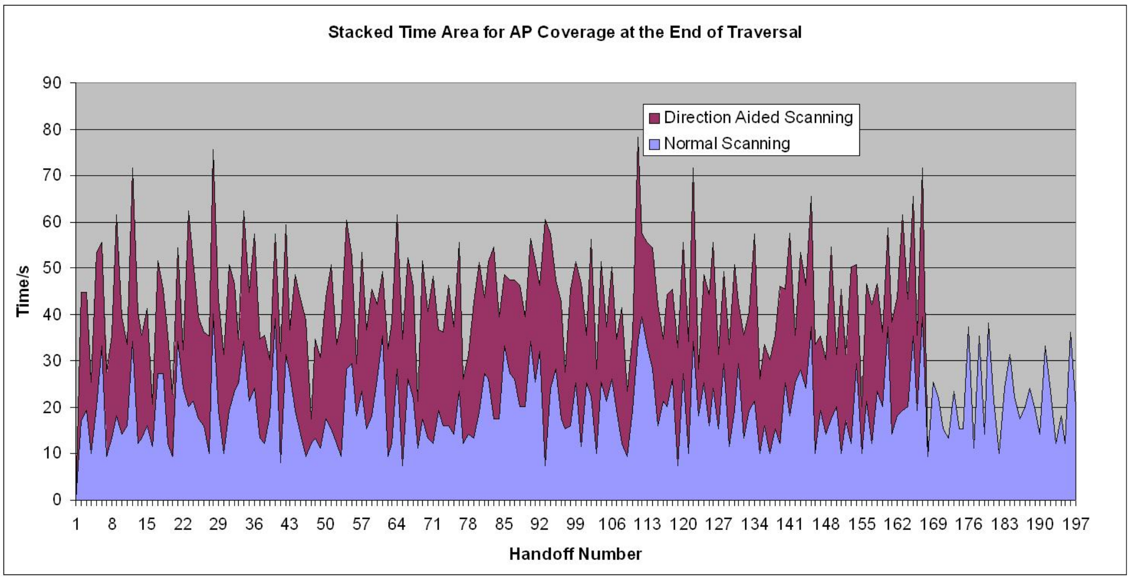


Figure 5.5: Stacked Time Area for AP Coverage when AP reaches Final Destination

Chapter 6

Conclusions

University of Cape Town

This dissertation addressed the problem of a mobile node incurring latency by scanning all frequency channels at the link layer level when it undergoes handover. Users of mobile devices expect to have seamless operation during handovers from one 802.11 AP to another. Current handover schemes are viewed as being insufficient to satisfy the real-time end-to-end delay tolerance of VoIP applications. To circumvent the lengthy Full scan process the dissertation presents two approaches. One approach called Single Channel scan allows for the mobile node to scan only one channel and hence reduce latency and signaling by a magnitude of eleven in the 802.11b protocol which supports eleven channels. The second approach which is the AP Response scan method further reduces the time by listening to the probe responses as they are received and breaking the scanning as soon as the correct response is received. This leads to the scanning process becoming as efficient as possible and taking up a minimal time of just over 1 ms on average. The architecture described in the dissertation outlines how the system works and the evaluation simulations show its effectiveness in WLANs.

In an attempt to minimise the scanning at layer two, the following conclusions based on our experience and evaluation in this dissertation have been drawn.

- The *MaxChannelTime* is important to the scanning because it determines how long a mobile node should stay in the frequency channel that it is scanning. If the *MaxChannelTime* is too low, it will miss some probe responses, and if it is too high, it will stay too long in frequency channels after receiving all probe responses and effectively cause the mobile node to become inefficient.

- Handover latencies at the link layer are dominated by the scanning involved and an efficient system such as the one presented in this research can alleviate the latencies from incurring 90% of the time to only incurring the time for two messages; which are one probe response and one probe request.

- The link layer latencies obtained from our algorithms show that they would be more suitable for real-time traffic generation than other previously proposed solutions. This is because they take much less than 50 ms to complete the link layer handoff.

- The *SwitchingTime* involved is dependent on the manufacturing, but the proposed solutions evade the need for extra switching time latencies involved with switching between two or more channels if the expected AP exists in the single channel scanned.

- The use of localization in handover can be established in an outdoor and an indoor environment. Our dissertation outlines possible choices for localization techniques. We have specified that we simulate for an outdoor environment and hence our chosen localization technique is Assisted-GPS, since it suitable for outdoors and has accuracies of up to 1 meter.

- The direction of a mobile node is necessary in determining the best AP to choose at handoff and the guaranteeing the longest coverage by a chosen AP at all times.

- If future networks have moving subnets, then the position and direction of nodes together with the position and direction of the moving APs will become more vital in order to choose the best subnet for handoff.

University of Cape Town

Chapter 7

Recommendations

After completing the work done in this project, these are the recommendations for future work in this topic.

- The proposed system needs more testing in order to scrutinise the outcomes of how it performs when there are many obstacles in the environment which can block the GPS and WLAN signals.
- The effect of localization errors can be incorporated into the research to see whether the proposed system will have degraded performance.
- The solutions can also be attempted physically in an outdoor environment.
- Prediction algorithms such as Deep Mining can also be included to aid the direction algorithms thus adding surety and guaranteeing successful handoffs to a moving mobile node.

University of Cape Town

Bibliography

[1] Albert Cabellos-Aparicio, René Serral-Gracià, Loránd Jakab and Jordi Domingo-Pascual. Measurement Based Analysis of the Handover in WLAN MIPv6 Scenario, Measurement. Springer Berlin / Heidelberg, Volume 3431/2005

[2] G. Dommety, Raj Jain. Potential Networking Applications of Global Positioning Systems. OSU Technical report, April 1996

[3] http://www.hummerlaptops.com/Hummer_datasheet2.pdf

[4] Arunesh Mishra , Minho Shin , William Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. ACM SIGCOMM Computer Communication Review, v.33 n.2, April 2003

[5] Minho Shin , Arunesh Mishra , William A. Arbaugh, Improving the latency of 802.11 hand-offs using neighbor graphs, Proceedings of the 2nd international conference on Mobile systems, applications, and services, June 06-09, 2004, Boston, MA, USA.

[6] Sangheon Pack. Hakyung Jung. Taekyoung Kwon. Yanghee Choi.SNC: A Selective Neighbor Caching Scheme for Fast Handoff in IEEE 802.11 Wireless Networks. Communications, 2005. ICC 2005. 2005 IEEE International Conference on, 16-20 May 2005.

[7] The GUI User Manual for the NCTUns 3.0 Network Simulator and Emulator

[8] N. Van den Wijngaert & C. Blondia. A Location Augmented Low Latency Handoff Scheme for Mobile IP. Proceedings of the First International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2004), Yokosuka, Japan, pp. 180-185, 2004.

[9] Vladimir Brik, Arunesh Mishra, and Suman Banerjee. Eliminating handoff latencies in 802.11 WLANs using multiple radios: Applications, experience, and evaluation. In Internet Measurement Conference 2005.

[10] Fengping Li, Helsinki: A study of mobility in WLAN. University of Technology, Telecommunication Software and Multimedia Laboratory.

University of Cape Town

[11] Johnson, D., Perkins, C. and J. Arkko, Mobility Support in IPv6, RFC 3775, June 2004

[12] John Scott Clemmensen Jr, Dr. Alfred L. Wicks, Dr. Charles F. Reinholtz, Dr. William T. Baumann, Design of a Control System for Multiple Autonomous Ground Vehicles to Achieve a Self Deployable Security Perimeter, Virginia Polytechnic Institute and State University, July 11, 2007.

[13] http://forskningsnett.uninett.no/wlan/ieee80211x.html

[14] A. Mishra, M. Shin, and W. Arbaugh, .Context caching using neighbor graphs for fast handoffs in a wireless network,. In Proceedings of the IEEE Infocom Conference, Hong Kong, China, March 2004.

[15] Gurpal Singh, Ajay Pal Singh Atwal, and Dr. Balwinder Singh Sohi. A Neighborhood Awareness Method for Handoff Assistance in 802.11 Wireless Networks. The Third International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2006), October 11 - 13, 2006 BCS London Office, London, U.K.

[16] Hye-Soo Kim, Sang-Hee Park, Chun-Su Park and al. .: Selective Channel Scanning for Fast Handoff in Wireless LAN using NeighborGraph. The 2004 International Technical Conference on Circuits/Systems Computers and Communications (ITC-CSCC2004) Japan, July 2004.

[17] Weatherspoon S. Overview of IEEE 802.11b Security, Intel Technology Journal Q2, Network Communications Group, Intel Corporation 2000.

[18] K. Ramachandran, S. Rangarajan and J. C. Lin. Make-Before-Break MAC Layer Handoff in 802.11 Wireless Networks. Proceedings of IEEE International Conference on Communications (ICC 2006), Turkey.

[19] A. M. Houyou, H. De Meer, M. Esterhazy. P2P-based Mobility Management for Heterogeneous Wireless Networks and Mesh Networks. MIP-0501 report, presented at EuroNGI Joint Workshops on “Wireless and Mobility” (IA 8.3) and on “New Trends in Network Architectures and Services” (IA 8.2), July 13 - 15, 2005, 3883 Springer 2006, ISBN 3-540-34025-4, Menaggio Como, Italy.

[20] www.engim.com

[21] Mustafa Ergen. IEEE 802.11 Tutorial. UC Berkeley, June 2002.

[22] Ishwar Ramani and al. SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks. Proceedings of the IEEE INFOCOM Conference, Miami, March 2005.

University of Cape Town

[23] A. Hasson, N. Ventura and S. Shepstone. Mobile IP Movement Detection Optimizations in 802.11 Wireless LANs. 1st International Symposium on Wireless Communication Systems 2004, Proceedings 20-22 September 2004 MAURITIUS

[24] Sangho Shin, Andrea Forte and Henning Schulzrinne Seamless Layer-2 Handoff in IEEE 802.11 Wireless Networks using Two Radios, Tech Report.www1.cs.columbia.edu/~ss2020/papers/dualcards.pdf

[25] S. Shin, A. Forte, A. Rawat and H. Schulzrinne Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs, In Proceeding of ACM MobiWAC (2004).

[26] A. Saleh, A location-aided decision algorithm for handoff across heterogeneous wireless overlay networks. Master's thesis, Virginia. Polytechnic Institute and State University, 2004.

[27] Mustafa Ergen, Sinem Coleri, Baris Dundar, Rahul Jain, Anuj Puri, Pravin Varaiya, Application of GPS to Mobile IP and Routing in Wireless Networks. Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th, Publication Date: 2002, Volume: 2, on page(s): 1115- 1119 vol.2

[28] Juuso Pesola, Sami Pönkänen, Location Aided Handover in Heterogeneous Wireless Networks. Wireless Personal Communications: An International Journal, Volume 30 ,Issue 2-4 (September 2004), Pages: 195 – 205, Year of Publication: 2004

[29] Héctor Velayos and Gunnar Karlsson . Techniques to Reduce IEEE 802.11b MAC Layer Handover Time. KTH Technical Report TRITA-IMIT-LCN R 03:02, ISSN 1651-7717, ISRN KTH/IMIT/LCN/R-03/02–SE, Stockholm, Sweden. April 2003

[30] http://www.trimble.com/ms750.html

[31] http://www.laipac.com/gps_tf30cf_eng.htm

[32] http://www.gpscity.com/cat-laptop-gps.htm

[33] http://www.hummerlaptops.com/technologies.htm

[34] S.Y. Wang, C.L. Chou, C.H. Huang, C.C. Hwang, Z.M. Yang, C.C. Chiou, and C.C. Lin. The Design and Implementation of the NCTUns 1.0 Network Simulator. Computer Networks, Vol. 42, Issue 2, June 2003, pp. 175-197

University of Cape Town

[35] Daniels, R. C., and Huxford, R. (2001). Using GPS: How It Works, Limitations, and Some Guidelines for Operation. Washington Department of Ecology. http://www.ecy.wa.gov/pubs/0006015.pdf. Accessed September 12, 2001.

[36] http://nsl10.csie.nctu.edu.tw/

[37] Nissanka B. Priyantha, Anit Chakraborty, Hari Balakrishnan, The Cricket Location-Support system, Proc. 6th ACM MOBICOM, Boston, MA, August 2000.

[38] Tian He , Chengdu Huang , Brian M. Blum , John A. Stankovic , Tarek Abdelzaher, Range-free localization schemes for large scale sensor networks, Proceedings of the 9th annual international conference on Mobile computing and networking, September 14-19, 2003, San Diego, CA, USA

[39] Sameer Tilak, Vinay Kolar, Nael B. Abu-Ghazaleh and Kyoung-Don Kang. Dynamic Localization Protocols for Mobile Sensor Networks. IEEE IWSEEASN 2005.

[40] Peterson, J.A Presence-based GEOPRIV Location Object Format, draft-ietf-geopriv-pidf-lo-03 (work in progress), September 2004.

[41] Want R., Hopper A., Falcao V., and Gibbons J. The Active Badge Location System. ACM Transactions on Information Systems 10, 1 (January 1992), 91–102.

[42] Hazas, M. and Ward, A. A Novel Broadband Ultrasonic Location System. In Proceedings of UbiComp 2002: Fourth International Conference on Ubiquitous Computing, Lecture Notes in Computer Science volume 2498, pages 264-280, Gorg, Sweden, September 2002.

[43] Deeya S. Nursimloo, George K. Kalebaila and H. Anthony Chan, A Two-Layered Mobility Architecture Using Fast Mobile IPv6 and Session Initiation Protocol. EURASIP Journal on WIreless Communications and Networking. Volume 2008, Article ID 348594.

University of Cape Town

Appendix A - Different Scanning Algorithms

A1. Channel Mapping Scheme

University of Cape Town

A mobile node performs a full scan for the first time when the wireless device is turned on. From the full scan, a channel mask is created by flagging the channels in which a Probe Response was received and also flagging channel 1, 6 and 11 as these channels are more likely to be used by APs. After that, the device selects the best AP by connecting to the AP with the best signal strength from the scanned set of APs. The channel in which the selected AP is in is removed from the channel mask by unflagging the corresponding bit, since the likelihood of an adjacent AP on the same channel as the current AP is very small. The channel mask used in the next handoff to reduce the amount of unnecessary time spent on probing non-existent channels among neighbouring APs becomes:

[Channels scanned at full scan + channel 1 + channel 6 + channel 11 – current channel]

If the channel mask does not result in an AP being found at the next link layer scan, the mobile node does a full scan again to create a new channel mask.

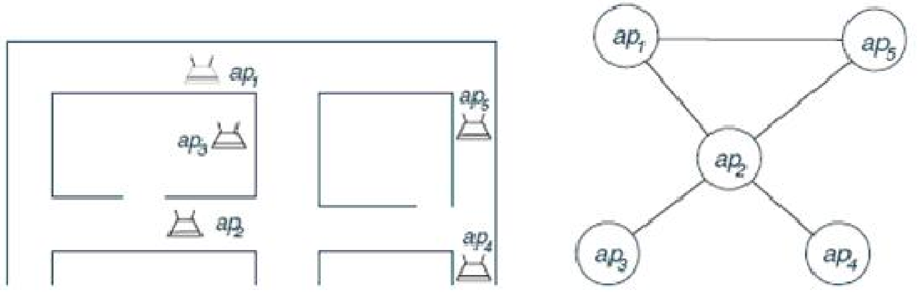
The cache mechanism is used to further reduce the handoff delay. It does this by storing the handoff history of the mobile node. With each AP that the mobile node associates with, a cache entry of that AP is inserted into the cache. When the handoff is about to happen, the mobile node first checks its cache for the MAC address of the current AP. If there is a corresponding cache entry, the mobile node does not even scan but simply associates to the correspondent AP. Further details of the implementation of the Channel Mapping Scheme can be obtained from [25].

A2. Neighbour Graphs Algorithms

A2.1 Abstracting the NG

The ordinary NG algorithm abstracts the hand-off relationships between the different APs. Using NG, the channels where neighbouring APs are currently operating can be learned. With this information, a mobile node can determine whether a channel needs to be probed or not [6].

Two APs are considered non-overlapping if the mobile node cannot communicate with both of them with acceptable link quality. This means that, if the mobile node received a probe response frame from APi, and APi is non-overlapping with APj, the mobile node cannot receive a probe response message from APj. Using NG-pruning, the mobile node can prune some of the APs that are non-overlapping with the AP groups that have already responded from the waiting group. Given a placement of APs shown in figure 1(a), the NG process creates a corresponding NG that is depicted in figure 1(b)



(a) (b)

Figure 1: (a) placement of APs (b) corresponding NG.

A2.2 Implementing the NG

There are various ways of implementing the neighbour graph: the user-oriented, the centralised and the distributed way [5]. In the user-oriented method of implementing Neighbour Graphs, each user keeps a track of their own Neighbour Graph, whereas in the centralised method, the Neighbour Graph is stored at a NG-server and handoff events are reported by APs. To get the information of AP relationships, a mobile node communicates with this NG-server via the current AP. The APs alert the NG-server of new neighbour APs in order to keep it up to date. In the distributed method, each AP stores its own local Neighbour Graph and mobile nodes obtain this information once they are associated to the AP. There are two ways that APs can learn the edges in the graph. The first one is when an AP receives an 802.11 re-association request frame from a mobile node; the message contains the MAC (BSSID) of the old-AP and hence establishes the re-association relationship between the two APs. The second method of learning new edges is through receipt of a Move-Notify message from another AP via the Inter Access Point Protocol (IAPP) [23]. In order to remove edges between APs from the cache, each AP performs a Least Recently Used (LRU) algorithm [14]. This method of removing APs using LRU is problematic since potential APs can be evicted because of other clients making more re-associations at other neighbouring APs. The distributed method also introduces cache misses because of re-associations between non-neighbour APs [14].

A2.3 SyncScan

SyncScan or Synchronised Scanning has been suggested as another way to minimise handoff latency [22]. The basic algorithm of SyncScan is that all APs on channel 1 will broadcast their beacons at time t, while APs on channel 2 will broadcast their beacons at time $t + d$, and channel 3 APs will send their beacons at time $t + 2d$, and so on. If a mobile node is operating on channel c, it can detect APs operating on channel $c + 1$ by switching to that channel d ms after it gets a beacon from the current AP. The mobile node must operate in the passive mode of scanning while doing this. For SyncScan to work efficiently, all APs that the mobile node might potentially handoff to must be known, and furthermore they must be adjusted so that all APs in one channel broadcast at the same time after d ms.

Complications that are eminent with SyncScan are the drift in timing accuracies over long intervals at the APs, and the problem of interference when all APs in the same channel broadcast their beacons at the same time [22]. Another problem with SyncScan is that while a mobile node switches from one channel and starts to listen passively on another channel, it cannot be sending or listening to its own AP [22].

University of Cape Town

A2.4 MultiScan

MultiScan reduces handoff latencies in 802.11 to zero seconds by using multiple radio cards [9]. As shown in figure 2, the mobile node is equipped with two wireless cards. The card that is currently associated to an AP (Card A) is the primary interface and the second card is the secondary interface (Card B). When Card A experiences deterioration in its signal strength, the secondary interface performs a normal full scan and connects to a new AP. After that, an interface switch occurs whereby the outgoing traffic of the mobile node is sent via the secondary interface. In this way, the secondary

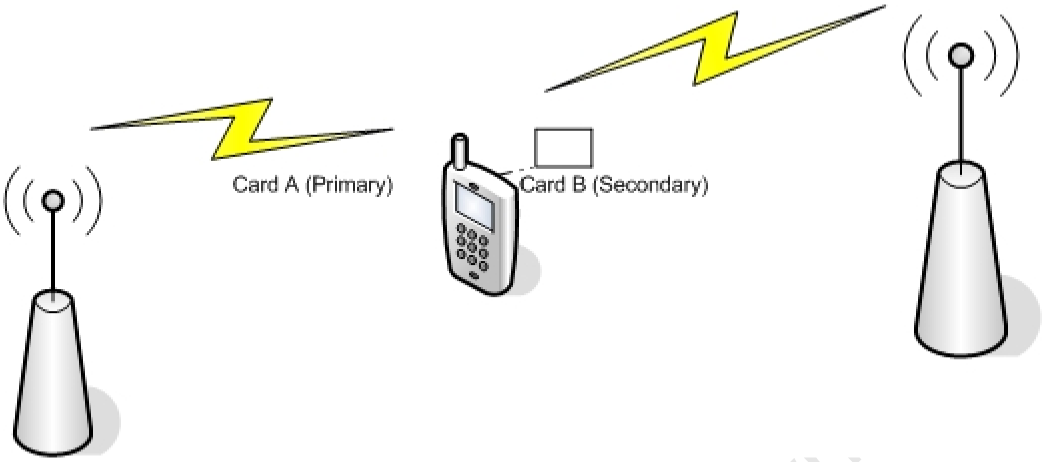


Figure 2: MultiScan Operation

interface becomes the primary interface and the primary interface becomes the secondary interface until another switch.

MultiScan operation effectively eliminates the handoff times. There already exists multi-band 802.11 chipsets that allow communication on two or more channels (e.g. EN-3001 intelligent wideband WLAN chipset for 802.11 networks) [20]. The problem with MultiScan is that the two interfaces could potentially interfere with each other's radio ranges and lead to an even poorer performance. This cross-interference would be experienced more with small form factors such as PDAs or a handset [9]. Even if the two interfaces are operating on different channels, they can still experience interference because only three non-interfering channels exist in 802.11b [21]. Another potential problem with MultiScan is that packets already queued on the primary interface will be lost if the old AP learns that the node is associated with a different AP and will no longer accept the nodes packets. This can happen if the primary interface's channel is much more congested than the secondary interface's channel [9].

University of Cape Town

Appendix B - Indoor Localization Techniques

University of Cape Town

B1. Infrared Signals - Active Badge System

The Active Badge system was originally designed as an emergency locator for personnel in large establishments such as hospitals. The system can also be useful to locate mobile users indoors and is very accurate [42]. In Active Badge, the item to be tracked is equipped with a tag called an "Active Badge". This tag emits a unique code for a tenth of a second at a given period (a beacon). Sensors placed in the host building pick up the unique identifiers and relay these to a master location manager. Pulse-width modulated infrared (IR) signals are used for signalling between the badge and sensor. This means that a mobile node can be tracked and the location manager can easily identify APs that are closest to the mobile node as it moves. The location manager can then be in a position to alert the mobile node, via the current AP of which AP is best for its next handoff.

Infrared (IR) signal are signals that do not suffer from synchronization problems and have already been exploited commercially (e.g. remote control in domestic appliances), hence it can be made very small and made very cheaply [42]. Active Badge IR signals however, suffer from not being able to transmit through walls. If there are enough sensors, this problem can be solved because even if a signal reflects from walls, it can be picked up by another sensor in the building after reflecting. Another problem is that the transmitted signal consumes power meaning that the signalling rate is an important design issue [42]. It also performs poorly in the presence of sunlight, and incurs installation and maintenance costs.

B2. Ultrasonic Localization

Ultrasonic location techniques are based on measurements of time-of-flight of sound pulses from an ultrasonic mobile node transmitter to receivers placed at known positions in an indoor area. The distance is calculated between the transceiver and receiver and through multilateration; the transmitter's position is calculated. In the example of [41], the transmitter operates at a frequency of 418 MHz and sends pulses every 200 ms. The location sensors are low powered and of low-cost [41].

B3. Cricket

An example of an ultrasonic location system is Cricket. In Cricket, beacons are used to distribute information to listeners in a certain indoor space. A beacon is a small device that is attached to some location within the geographic space it advertises in. These beacons are inexpensive and more than one of them can be used in a space [37]. They are mounted on walls and the ceiling and they emit RF signals along with concurrent ultrasound pulses. Upon receiving the RF and ultrasound pulse, the listener then correlates them together and gets an estimation of where it is in the space. Cricket has an accuracy of 6 cm [43].

B4. BAT System

Another ultrasonic localization technique is the Bat system where users wear small badges, which emit an ultrasonic pulse when radio-triggered by a central system. The system determines pulse times-of-light from the badges to a network of receivers on the ceiling, and uses a multilateration algorithm to calculate the 3D positions of the badges. The system yields location information with an accuracy of approximately 3 cm [43].

B4. Constellation System

The best of the ultrasonic localization techniques so far is the Constellation system which tracks a mobile unit that has a 3D inertial sensor and a number of ultrasonic sensors. Location is calculated using time-of-light measurements between the mobile node and the transmitters in the environment. An accuracy of approximately 5 mm is achieved [43].

University of Cape Town

Appendix C - AP Coordinates in our Simulations:

Cape Town

Table 1: AP Coordinates for the Full versus Selective Scanning Simulation Environment

APID	X-Coordinate	Y-Coordinate
5	629.000000	439.000000
6	863.000000	434.000000

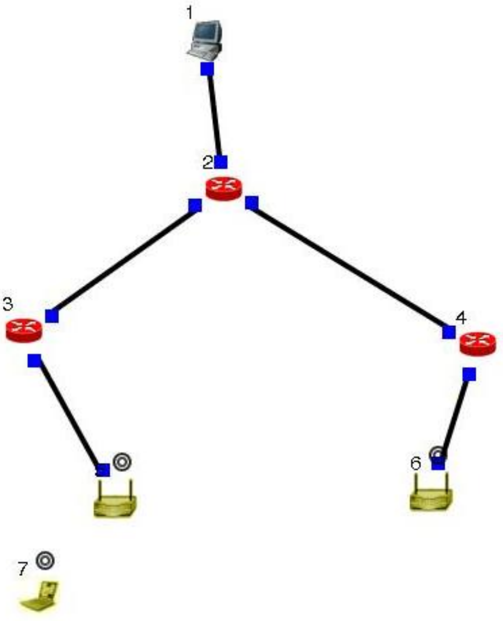


Figure 3: Actual View of APs from NCTUns 4.0

Table 2: AP Coordinates for the Direction Aided Simulation Environment

APID	X-Coordinate	Y-Coordinate
6	413.000000	670.000000
7	681.000000	520.000000
8	980.000000	980.000000
10	617.000000	628.000000
11	576.000000	215.000000
12	486.000000	438.000000
13	671.000000	268.000000
14	305.000000	482.000000
15	836.000000	388.000000
16	781.000000	502.000000
17	1068.000000	613.000000
18	579.000000	448.000000
19	877.000000	545.000000
20	353.000000	220.000000
21	839.000000	198.000000
22	1090.000000	259.000000
23	1241.000000	422.000000
24	826.000000	671.000000
25	606.000000	752.000000
26	1204.000000	570.000000
27	970.000000	234.000000
28	398.000000	342.000000

University of Cape Town

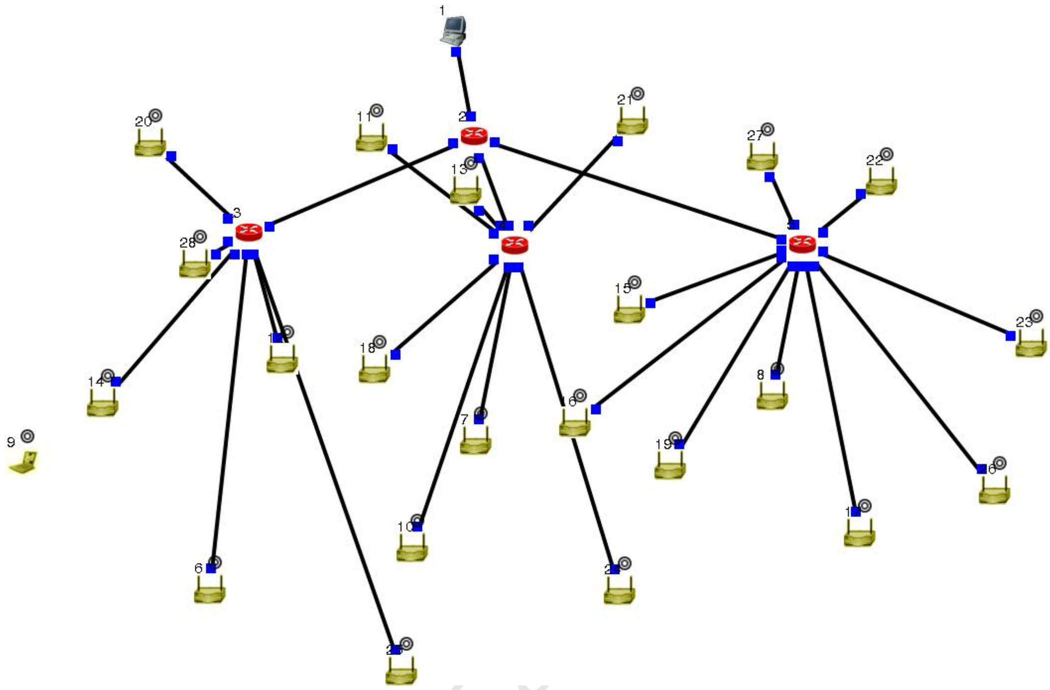


Figure 4: Actual View of Direction Aided Simulation from NCTUns 4.0

University of C

Appendix D - Mobile Node Movement per Simulation

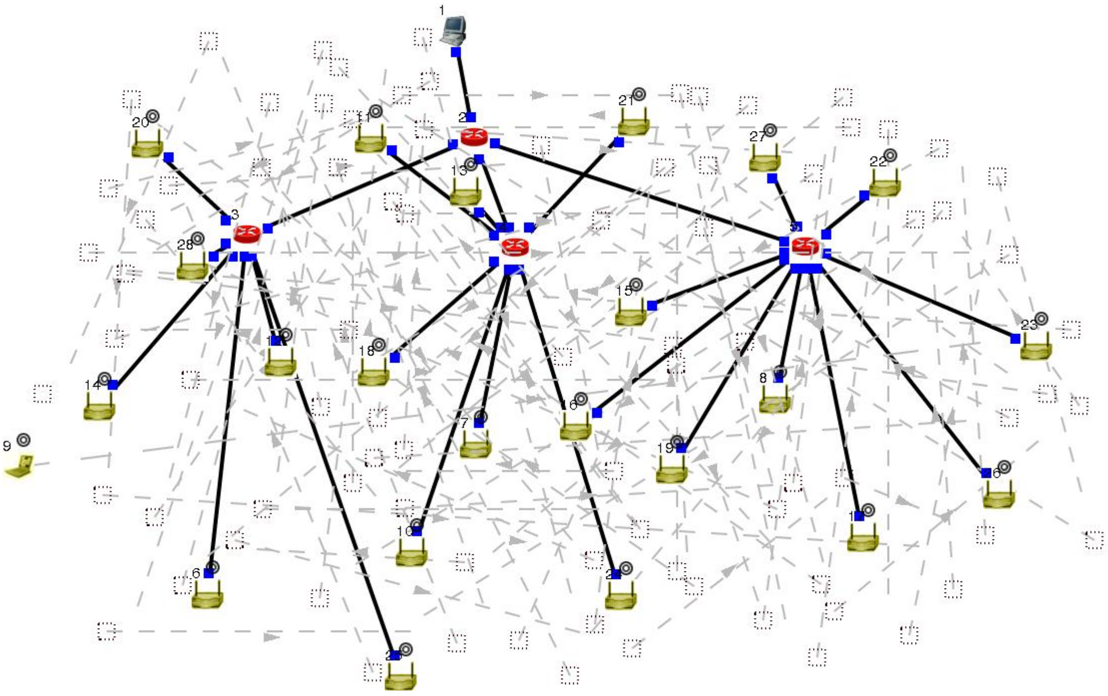


Figure 5: Actual Movement of Mobile Node for Direction Aided Scanning

Appendix E - Overview of Mobile IP

University of Cape Town

Mobile IP (MIP) happens when a mobile node moves into a new subnet and acquires what is known as the Care-of Address (COA). The steps involved during MIP are link layer handoff, movement detection and registration. Mobile IP introduces two communication entities called the Home Agent (HA) and the Foreign Agent (FA) [10]. The total involved entities are the Corresponding Node (CN), Mobile Node (MN), Home Agent (HA) and Foreign Agent (FA). These entities work together to assist a mobile node when it is moving across different Basic Service Stations (BSS) and Extended Service Stations (ESS) . Mobile IP therefore relies on these 4 entities in order to perform the task of handoffs. Two versions of MIP that have been released so far are the MIPv4 and the MIPv6. MIPv4 was released to work with Internet Protocol version 4 (IPv4) and MIPv6 is an extension of IPv6.

E.1 Mobile IP Operation

When a mobile node is connected to its home subnet, it gets its "home address". Its home address is similar to the (normally permanent) address that a host would have in an Ethernet. When in the home subnet, packets addressed to the mobile node are routed to it using normal internet routing mechanisms [10]. When the mobile node is away from the home subnet, it gets a temporal address. For example in figure 2.1 if the home subnet of MN1 is BSS 1, then when MN1 moves to BSS2, it gets a new address, the COA which attaches it to BSS2. After that, it registers this COA with its HA by sending a Binding Update (BU) to the HA. The HA then replies to MN1 with a Binding Acknowledgment (BA). The binding is an association between a mobile node's Home Address and its COA. This binding is logged and stored for a specified period at the HA.

When packets arrive at the HA that are destined for the mobile node, which is at the foreign network, the HA checks the binding and then forwards the data to the current COA of the mobile node. In MIPv4, the HA and FA construct a Bi-directional Tunnel (BET) in order to get the data to

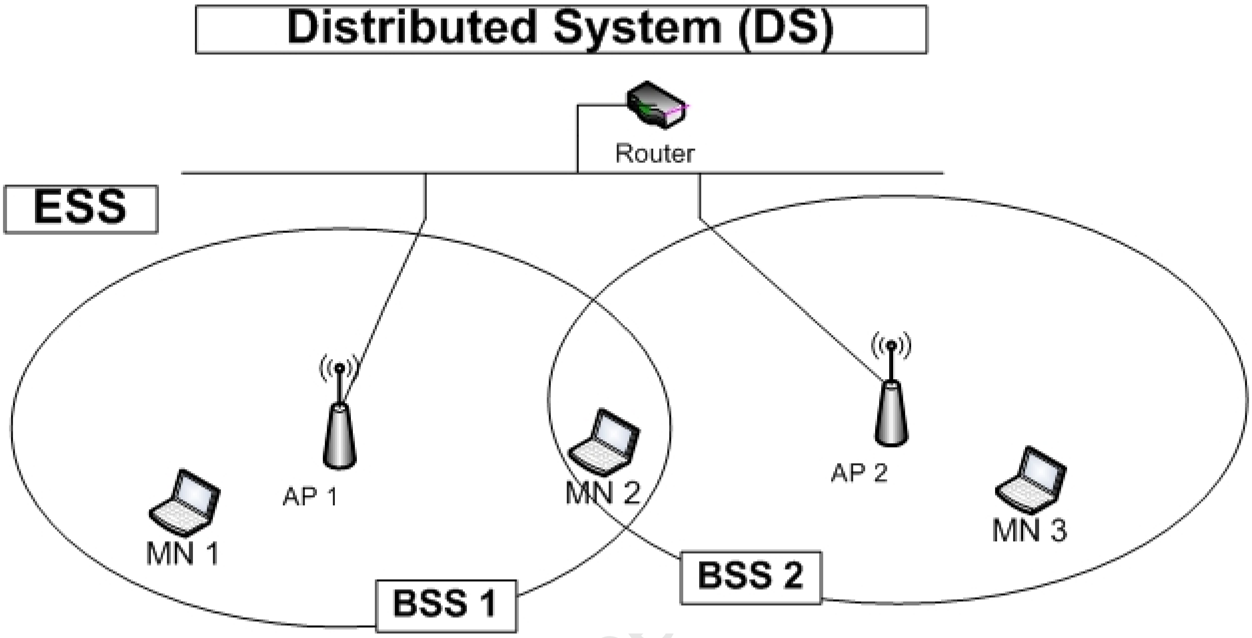


Figure 6: A Distributed System

the mobile node at the foreign subnet. The HA then operates as a proxy for packets coming from the CN that are addressed to the mobile node. This is called the triangular problem because packets have to go via the HA to get to the mobile nodes COA. In MIPv6 the operation is the same, the mobile node however can use the option of Route Optimization. When Route Optimization is turned on, the mobile node sends a BU to the CN. The CN then sends data straight to the COA and avoids going via the HA. Due to this, MIPv6 ends the triangular routing problem that exists in MIPv4 [10]. MIPv6 has many more improvements to MIPv4 which are however not relevant to this research [11].

University of Cape

Appendix F - Locations in NCTUns

API Name: GetNodeLoc(), GetNodeAntenna()

Synopsis: int GetNodeLoc(u_int32_t nid, double &x, double &y, double &z)

Return value: The return value of above functions is 1 for success and $<$ 0 for failure.

Description:

The GetNodeLoc() function gets the current position of a node. The returned information of a node position will be stored in the parameter ‘x’, ‘y’ and ‘z’. Each node in a simulation has its position information. This position information is updated periodically by the S.E in the simulator. When a simulation starts, the simulator reads a scenario file to create events to periodically update a node’s position. The syntax of the scenario file is shown as follows: $node_ (<node_id>) set <X > <Y> <Z> <arrival_time> <pause_time> <speed> The above syntax says that the node_id arrives at (X, Y, Z) position at time arrival_time at a speed of speed. Before moving next, the node will pause for the time specified in pause_time.

University of Cape Town

Appendix G - Accompanying CD

The accompanying CDROM is located on the inside back cover of this document. The contents of the CDROM are as follows:

- A soft copy of this thesis in PDF format.
- The NCTUns 4.0 source code used to run the simulation.
- The Results folder which has in it:
    - Exp1 folder to signify the Full versus Selective scanning results. In that folder there is:
        - An Excel file called "Exp1Latencies" which has the latencies of all three algorithms for Full versus Selective scanning.
        - A .mpt file which has the mobile node movements. Each line in this file represents a waypoint and its format is (X_pos, Y_pos, Arrival Time, Pause Time, Moving Speed). Wordpad may be used to view the file.
- The ScanningMethods folder which has the APResponse, SingleScan, and OriginalScan subfolders. Each folder has an implementation of its algorithm in the mobilenode.cc file.
- The SimulationFiles folder which contains the simulation files for Full versus Selective scanning are in the Exp1 folder and in the Exp2 folder for Direction Aided scanning.

University of Cape Town