

VERTICAL HANDOFF BETWEEN 3G NETWORKS AND WLANS

by

Feng Zhang

Submitted in partial fulfillment of the requirements
for the degree of Master of Computer Science

at

Dalhousie University
Halifax, Nova Scotia
December 2005

© Copyright by Feng Zhang, 2005



Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 978-0-494-16557-7

Our file Notre référence

ISBN: 978-0-494-16557-7

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.


Canada

DALHOUSIE UNIVERSITY

To comply with the Canadian Privacy Act the National Library of Canada has requested that the following pages be removed from this copy of the thesis:

Preliminary Pages

Examiners Signature Page (pii)

Dalhousie Library Copyright Agreement (piii)

Appendices

Copyright Releases (if applicable)

To my wonderful parents

Zhang Shun Cheng and Lv Xiu Lan

Table of Contents

Abstract.....	XI
Acknowledgements.....	XII
Chapter 1. Introduction.....	1
1.1. Research Background.....	1
1.2. Earlier Research on Vertical Handoff.....	3
1.3. Thesis Outline.....	8
Chapter 2. Technology Background.....	10
2.1. WCDMA and UMTS Radio Access.....	10
2.1.1 Physical Layer.....	11
2.1.2 Media Access Control.....	12
2.1.3 Radio Link Control.....	13
2.1.4 Packet Data Convergence Protocol.....	13
2.1.5 Radio Resource Control Protocol.....	14
2.1.6 Radio Resource Management.....	14
2.1.6.1 Power Control.....	14
2.1.6.2 Congestion Control.....	15
2.1.6.3 Resource Management.....	17
2.2. WLAN Radio Access.....	17
2.2.1 System Architecture.....	17
2.2.2 Physical Layer.....	19
2.2.3 Media Access Control.....	20
2.2.4 Layer Management.....	23
2.3. Location Based Service.....	24
2.3.1 3GPP LCS Architecture.....	24
2.3.2 3GPP Positioning Method.....	25
2.3.3 WLAN Positioning method.....	27
Chapter 3. Handoff Algorithms.....	28
3.1. Cellular Basic.....	28

3.2.	Handoff.....	30
3.3.	Handoff Algorithms.....	32
3.3.1	Strength Based Algorithm.....	32
3.3.2	Other Handoff Algorithms.....	33
3.3.3	Emerging Handoff Algorithms.....	34
3.4.	WCDMA Handoff.....	35
3.4.1	Hard Handoff.....	35
3.4.2	Soft and Softer Handoff.....	36
3.4.3	Intersystem Handoff.....	38
3.5.	WLAN Handoff.....	40
3.6.	Vertical Handoff.....	44
Chapter 4.	Proposal.....	46
4.1.	Basic Idea of Location Aided Handoff.....	46
4.2.	System Architecture.....	48
4.3.	SRNC Handoff Decision.....	56
4.3.1	Handoff Prediction.....	56
4.3.2	Handoff Evaluation.....	61
4.4.	UE Signal Detection.....	63
4.5.	UE Handoff Decision.....	65
4.6.	Simulation.....	67
4.6.1	The Number of Handoffs.....	68
4.6.2	Battery Consumption.....	71
4.6.3	Call Drop Rate and Handoff Delay.....	72
4.6.4	Advantage of Road Topology.....	73
Chapter 5.	Conclusion and Future Work.....	75
Reference.		76

List of Figures

1	Comparison of Different Mobile Technologies.....	2
2	Wireless Overlay Network Structure.....	4
3	Horizontal and Vertical Handoff.....	4
4	Mark Stemm's Handoff System Architecture.....	5
5	Network Stack in Mark Stemm's Handoff System.....	5
6	Tightly Coupled and Loosely Coupled Architecture.....	6
7	Roaming Model - 3GPP PS Based Services Provided via Home Network.....	7
8	Roaming Model - 3GPP PS Based Services Provided via Visited Network.....	8
9	UMTS Architecture.....	10
10	Radio Interface Protocol Architecture.....	11
11	RRC Layer Architecture.....	14
12	IEEE 802.11 Architecture.....	19
13	ISO/IEC Basic Reference Model Covered in 802.11.....	19
14	Functions of PHY of 802.11b.....	20
15	802.11 MAC Architecture.....	22
16	Architecture of UE Positioning in UTRAN.....	27
17	Path Loss, Shadowing and Multi-path versus Distance.....	30
18	WCDMA Soft Handoff Algorithm.....	39
19	Handoff from GSM to UTRAN.....	41
20	Handoff in 802.11.....	42
21	AP Architecture with IAPP.....	44
22	System Architecture for Vertical Handoff.....	51
23	UE Initialized Downward Handoff.....	52
24	Network Initialized Handoff.....	53
25	Successful Network Initialized Downward Handoff.....	54
26	No Requirement for Downward Handoff.....	55
27	WLAN Signal Detection Failure.....	56
28	Network Initialized Upward Handoff.....	57

29	Using Pedestrian Road Map for Handoff Prediction.....	57
30	Flow Chart of Handoff Prediction algorithm.....	60
31	Flow Chart of Handoff evaluation algorithm.....	63
32	Signal Detection.....	64
33	Flow Chart of Signal Detection Algorithm.....	65
34	WLAN Signal Simplified Simulation.....	68
35	UE Moving Path.....	69
36	Number of Handoff.....	70
37	Number of Handoff in Transition Area.....	66
38	Battery Consumption.....	71
39	Drop Call Rate, Handoff Delay vs. UE Speed.....	73
40	Advantage of the Road Topology.....	74

List of Abbreviations and Symbols Used

3G	Third Generation
3GPP	Third Generation Partnership project
A-GPS	Assisted Global Positioning System
AP	Access Point
AMC	Adaptive Modulation and Coding
BSS	Basic Service Set
CN	Core network
DS	Distribution System
ESS	Extended Service Set
FDD	Frequency Division Duplex
HC	Handoff Control
GSM	Global System for Mobile Communications
GPRS	General Packet Radio System
GPS	Global Position System
HARQ	Hybrid Automatic Request
IBSS	Independent BSS
LCS	Location Service
LLC	Logic Link Layer
LMU	Location-management unit
MAC	Medium Access Control
MMS	Multimedia Messaging Services
MIMO	Multiple-Input Multiple-Output
O-TDOA	Observed Time Difference Of Arrival
PDCP	Packet Data Convergence Protocol
PLME	Physical Layer Management Entity
PMD	Physical Medium Dependent
PC	Power Control
BMC	Broadcast/Multicast Control
RLC	Radio Link Control
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
RRM	Radio Resource Management
RM	Resource Management
RSS	Received Signal Strength
SMLC	Serving Mobile Location Center
SNR	Signal to Noise Ratio
SRNC	Serving Radio Network Controller
SAS	Stand-Alone SMLC
SMS	Short Message Services

STA	Terminal Station
TDD	Time Division Duplex
U-TDOA	Uplink Time Difference of Arrival
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UTRAN	UMTS Terrestrial Radio Access Network
WLAN	Wireless Location Area Network
WCDMA	Wideband Code Division Multiple Access
HSDPA	High Speed Downlink Packet Access

Abstract

Next generation wireless networks will be heterogeneous. 3G cellular networks provide worldwide coverage, while wireless LANs can be deployed to get high bandwidth Internet access in hotspots. These two kinds of wireless networks are complementary and should be integrated to make sure that subscribers can always be best connected to the networks. Vertical handoff, which maintains the connection active during switching between different access networks such as from a 3G network to a WLAN, is a critical problem for the integration of these two wireless technologies. The technique used for vertical handoff is much more complex than that of the corresponding horizontal handoff used in homogenous networks because it is a multi-criteria decision issue involving bandwidth, price, traffic load, application attributes, battery status, signal quality and user preference. Also because vertical handoff uses much more network resources and results in longer delays, traditional ping-pong effects and the trade-off between the benefits and the negative aspects brought by handoff should be considered carefully. This thesis proposes a new location-aided architecture and algorithm for vertical handoffs between 3G networks and WLANs. A network-aided, handset controlled handoff architecture, which takes advantage of WLAN coverage maps, topology maps and the location information provided by 3G networks and WLANs is described. In addition, handoff prediction and evaluation algorithms and a multi-priority policy based decision making algorithm and signal detection algorithm are presented. Results of evaluation of the number of handoffs, battery consumption, drop cell rate and handoff delays are analyzed.

Acknowledgements

I would like to thank Prof. Srinivas Sampalli for his advice, knowledge and persistent encouragement during my study at Dalhousie University. Srinivas is a superb teacher, a great researcher and an excellent graduate coordinator. I was very fortunate in having the chance to work with him as my supervisor.

I would like to thank Dr. Jacek Ilow and Dr. Nur Zincir-Heywood for taking time to read my thesis and give me some insightful comment. I would also like to extend my thanks to Alex Petrovic and Fred Bullock who gave me a very nice job that supported me to finish my thesis.

Finally, I want to dedicate this thesis to my parents for their love, warmth, and support throughout.

Chapter 1

Introduction

1.1 Research Background

There are two kinds of wireless networks: cellular networks and wireless LANs (WLANs). Global System for Mobile Communication (GSM) and Wideband Code Division Multiple Access (WCDMA) are the representatives of cellular networks. Although the second generation (2G) mobile system, such as GSM, has successfully met voice communication needs, its data transmission rate is only 9.6-14.4 kb/s [1], which cannot support the fast increasing data services like Short Message Services (SMS), Multimedia Messaging Services (MMS) and mobile video and broadcasting. General packet radio service (GPRS), i.e., 2.5G mobile system, is based on the GSM infrastructure, but with higher data speed (average speed of 30 – 40 kbps and peak data rate of 115 kbps) [3]. GPRS provides the most ubiquitous wireless data service in the world right now. The third generation (3G) mobile system is based on code-division multiple access (CDMA). WCDMA provides 220 - 320kbps average data rate and 2Mbps peak downlink speed for current devices [2]. High Speed Downlink Packet Access (HSDPA) is a tremendous improvement on WCDMA. HSDPA can reach average data rate of 550-1100kbps and peak rate of 14.4Mbps for downlink by using Adaptive Modulation and Coding (AMC), Multiple-Input Multiple-Output (MIMO), Hybrid Automatic Request (HARQ), advanced receiver and fast cell searching technologies [3]. Figure 1 is a comparison of main cellular technologies.

Wireless LANs, which may be WiFi (IEEE 802.11), WiMax (802.16) or HIPERLAN/2 networks, is another fast growing communication technology. 802.11a and 802.11g provide the data rate up to 54Mbps with 100m radio coverage for outdoor environment and 30m for indoor environment [5]. WiMax provides the data rate up to 72Mbps with coverage up to 25-30km. 802.20 protocol is in progress, which is expected to give us a higher data rate and wider coverage. It is obvious that WLAN has a much higher data rate than cellular networks. Also, the cost of WLAN equipment, like Access Point (AP), is much cheaper than the Node Bs in 3G networks. To cover the same size

area, the overall cost of APs is still cheaper than Node Bs. In addition, surfing through WLAN is less expensive compared to the charge rate for 3G WWW service.

	Peak Network Downlink Speed	Average User Throughputs for File Downloads	Capacity	Other Features
GPRS¹³	115 kbps	30 – 40 kbps		
EDGE	473 kbps	100 – 130 kbps	Double that of GPRS	Backward compatible with GPRS
UMTS - WCDMA	2Mbps ¹⁴	220 - 320 kbps	Increased over EDGE for high-bandwidth applications	Simultaneous voice and data operation, enhanced security, QoS, multimedia support, and reduced latency
UMTS - HSDPA	14 Mbps ¹⁵	550-1100 kbps ¹⁶	Two and a half to three and a half times that of WCDMA	Backward compatible with WCDMA
CDMA2000 1XRTT¹⁷	153 kbps	50-70 kbps ¹⁸		
CDMA2000 1XEV-Data Optimized (DO)¹⁹	2.4 Mbps	300-500 kbps ²⁰		Optimized for data, VoIP in development

Figure 1. Comparison of Different Mobile Technologies [3]

Right now, WLANs are widely deployed in hotspots like airports, conference sites, office building, cafes, hotels and university campuses. However, it is not cost efficient to cover urban areas, let alone world wide areas like 3G networks. Other costs, such as that of backhaul links, cannot be ignored when the size of coverage areas is increasing [4]. The small radio coverage ability cannot make WLAN get the wide coverage benefit of 3G. Also, from perspective of security and mobility, cellular networks are much superior to the WLAN. In addition, cellular operators and many large mobile companies, who have large number of customers, have invested billions on the R&D of 3G /4G networks and will definitely not give up in this huge market. Pareek [4] says, “there is no clear winner, each technology supplements or complements the other.” 3G networks will be broadly deployed and provide services for subscribers anytime and anywhere, while WLANs will be used as an extension to 3G cellular networks in localized high-traffic-density areas. According to Doufexi’s simulation results in [6], the capacity and performance have been significantly increased when WLAN and 3G

networks are integrated. The integration of WLAN and WCDMA is the main topic in Release 6 of 3GPP technical specifications because 3GPP (3G Partnership Project) realizes that it is time to deploy another wireless access solution in hotspots to enable smooth access of corporate data services or meet the high bandwidth requirement of some applications (such as FTP, video conference and broadcasting, etc.).

Confidently we can reach a conclusion that the next generation wireless network will be heterogeneous. This means that it is important to devise mechanisms for vertical handoff for seamless transfer from one network to the other. Vertical handoff means that mobile terminal (cellular phone, PDA, etc) will make a handoff to 3G networks when the WLAN is not available; however, when the signals of WLAN are good enough, the terminal will switch back to WLAN to take advantage of the higher data rate and the lower price. Seamless means that the handoff procedure should be transparent to the subscriber and the application. The handoff decision algorithm should choose the optimal time and place to make a handoff in order to keep the mobile terminal always connected with the best networks. Seamless vertical handoff is a critical issue in beyond 3G or 4G wireless networks.

1.2 Earlier Research on Vertical Handoff

In 1998, Mark Stemm and Randy H. Katz proposed the concept of “vertical handoff”. In [10], they described the structure of wireless overlay networks (Figure 2), in which the lower level wireless networks, such as WLAN in buildings and campuses, have higher bandwidth and smaller coverage. The upper level wireless networks, such as metropolitan-area and regional-area mobile systems, have lower bandwidth and wider coverage.

Horizontal handoff is the traditional handoff, which happens between Node Bs, base stations or access points, using homogeneous wireless access interfaces. Vertical handoff is defined as the handoff between heterogeneous wireless networks. Figure 3 illustrates these two kinds of handoffs [10]. Vertical handoffs can be divided into two categories: upward and downward vertical handoff. An upward handoff is a handoff to a wireless network with larger cell size, while a downward handoff will make the mobile terminal connect with a smaller cell size network. It is obvious that a downward handoff

is not time-critical because mobile terminal can connect with upper wireless network without worrying about disconnection. The reason for downward handoffs is to get better service. On the contrary, upward vertical handoffs are time-critical because the connection will be terminated if the handoff decision and execution are delayed [10].

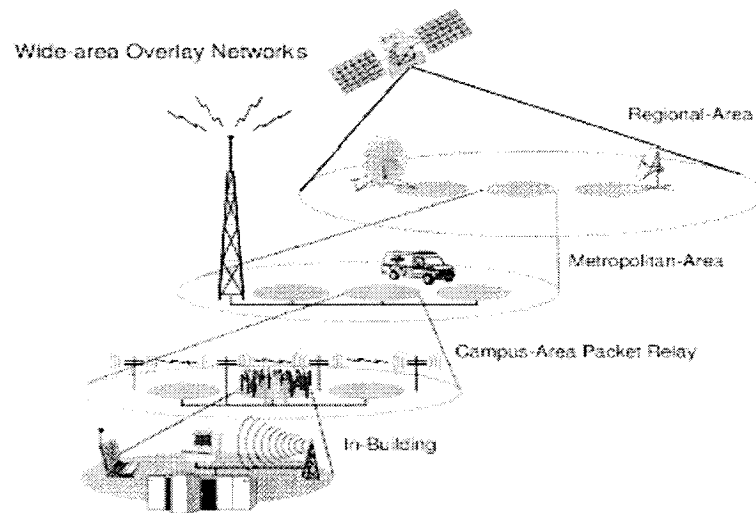


Figure 2. Wireless Overlay Network Structure [10]

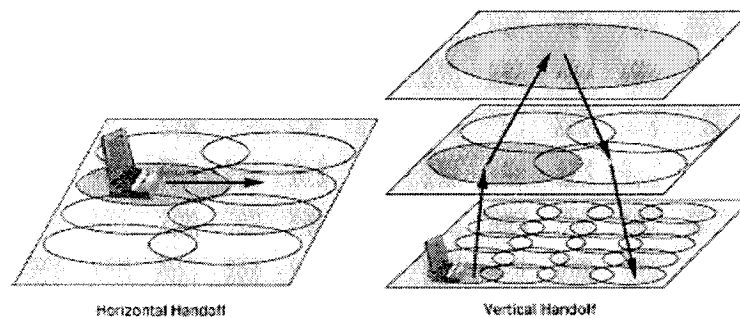


Figure 3. Horizontal and Vertical Handoff [10]

Stemm and Katz also defined the primary goals for seamless vertical handoff as: “low latency, power saving, minimized bandwidth overhead, optimal time to perform handoffs in unpredictable channels and service/system interoperability between commercial modals and technologies that cannot be improved” [10]. They also proposed an infrastructure, which is much similar to Mobile IP. Figure 4 is the architecture of their

vertical handoff system. The difference is that the care-of address is a multicast address instead of a unicast address in Mobile IP.

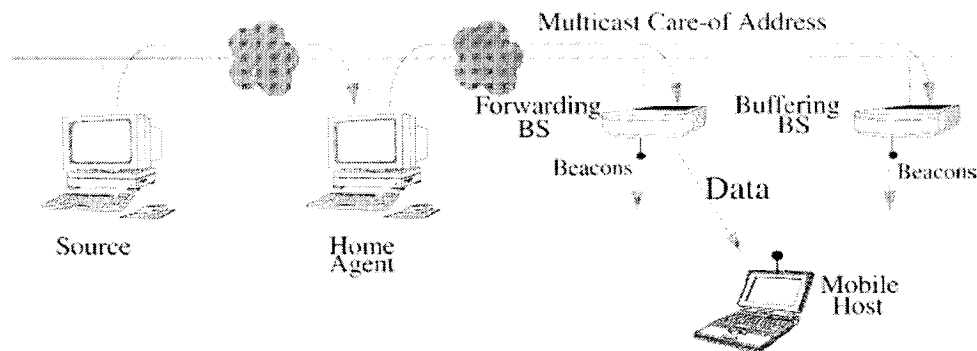


Figure 4. Mark Stemm's Handoff System Architecture[10]

Figure 5 shows the network stacks for the test bed used by Stemm and Katz. They also designed a simple algorithm for both downward and upward vertical handoff. The mobile terminal will always connect the network with the smaller cell as long as possible. Vertical handoff will be launched only when the currently connected networks do not have enough radio resources or strong enough signals.

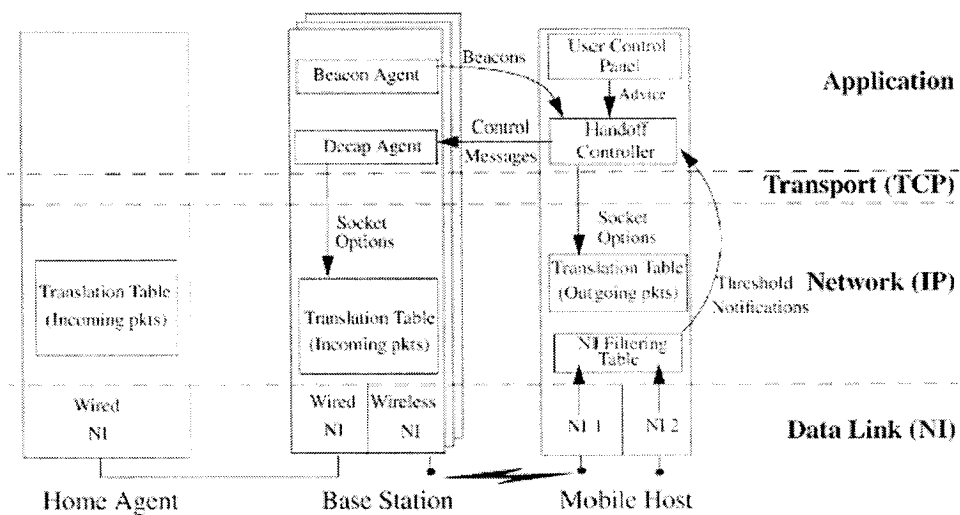


Figure 5. Network Stack in Mark Stemm's Handoff System [10]

The vertical handoff can be divided into two phases: handoff decision (when to handoff) and handoff execution (how to handoff). Right now most of the research is focused on the second phase, which includes the integration architecture and mobility protocol. Furthermore, much of the research is focused on the vertical handoff between 3G networks (either WCDMA or CDMA2000 based) and wireless LAN (802.11 based). Buddhikot [11] proposes two inter-working architectures for CDMA2000 based 3G networks and 802.11 based WLAN: tightly and loosely coupled architectures, which are illustrated in Figure 6. He recommends a loosely coupled architecture, which can “provide SimpleIP and Mobile-IP roaming services easily” [11]. He also discusses its detailed implementation, in which WLAN integration gateway was deployed to support seamless vertical handoffs. Salkintzis [12] proposes some WLAN/3G inter-working technologies and architectures that can support authentication, authorization, accounting, WLAN sharing and consistent service provisioning. Ahmavaara [13] outlines the usage of 3GPP subscription for WLAN access and introduces functionalities to implement 3GPP based access control and authentication. He also presents a user plane routing for accessing service. Faccin [14] investigates the issues regarding inter-working between SIP (Session Initiation Protocol) and Mobile IPv6. Wang and Abu-Rgheff [15] propose an integrated Mobile IP and SIP handoff management architecture, which can take advantage of the complementary abilities of these two IP protocols. In 3GPP TS 23.234 Release6, non-roaming and roaming WLAN inter-working reference models have been standardized. Figure 7 and Figure 8 are the roaming reference models for PS based service provided via home networks and visited networks.

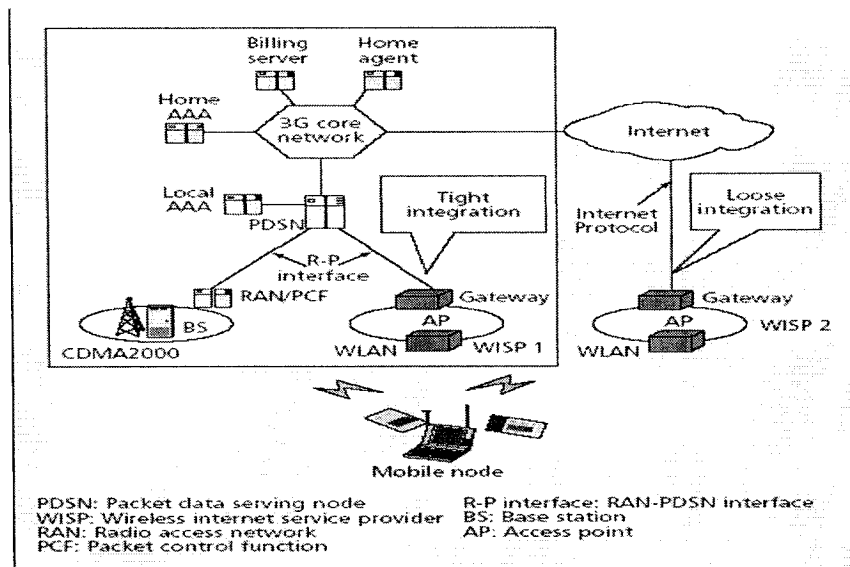


Figure 6. Tightly Coupled and Loosely Coupled Architecture [11]

Few publications on the handoff decision algorithm (the first phase of vertical handoff) can be found. The architecture and mobility protocol are open and will be standardized, but the handoff algorithm is proprietary [17], so the handoff algorithm is critical for wireless/mobile network companies. Wang [18] describes a policy-enabled handoff decision solution that allows user to define policy to make trade-off between bandwidth, power consumption and price and choose the best wireless access. Zhu [19] provides some optimization on the overall cost function by considering user preference and network conditions. Singh and Maturino-Lozoya and other researchers [20,21] propose a fuzzy logic based scheme to make multi-criteria vertical handoff decision. Zhang [22] identifies the handoff decision as a fuzzy multiple attribute decision making (MADM) problem and designs a MADM model for it. Pahlavan [17] suggests solving vertical handoff decision by using neural networks [17]. All of these publications just focus on the issue of multi-criteria decision and no complete solution for “when to handoff” has been proposed.

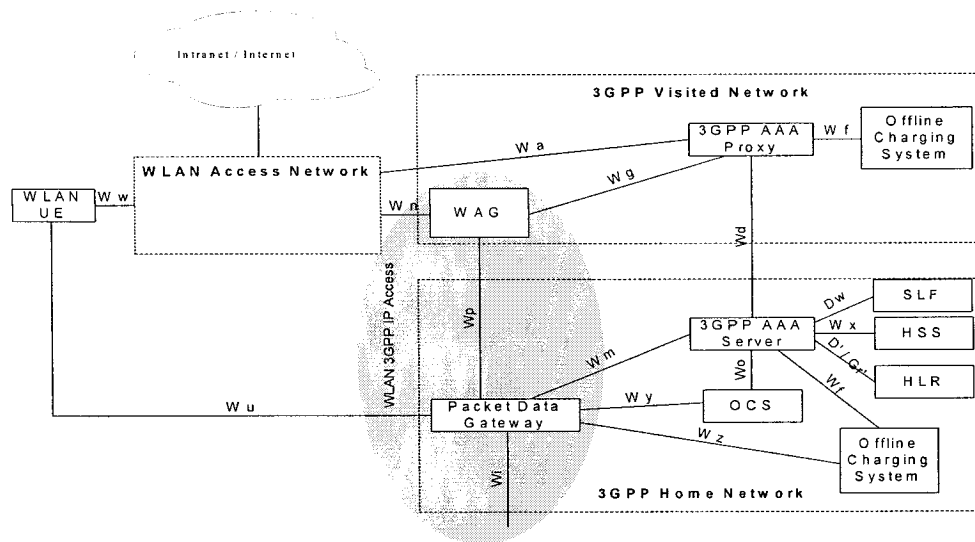


Figure 7. Roaming Model - 3GPP PS Based Services Provided via Home Network [16]

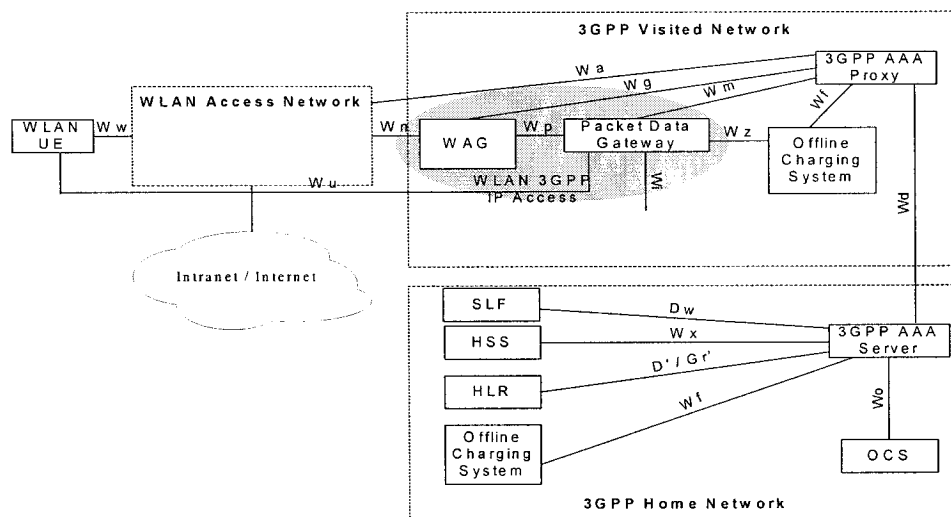


Figure 8. Roaming Model - 3GPP PS Based Services Provided via Visited Network [16]

1.3 Thesis Objective and Outline

The objective of this thesis is to propose a new location-aided architecture and algorithms for vertical handoffs between 3G networks and WLANs. A network-aided, handset controlled handoff architecture, which takes advantage of the WLAN coverage map, topology map and the location information provided by 3G networks and WLANs is

described. In addition, handoff prediction and evaluation algorithms and a multi-priority policy decision making algorithm and signal detection algorithm are presented. Results of evaluation of the number of handoffs, battery consumption, drop cell rate and handoff delays indicate the efficiency of this technique over non-location based schemes. Although we have chosen WCDMA based 3G technology and 802.11 protocols based WLAN technologies, the architecture and algorithms are also suitable for CDMA2000/TD-SCDMA based 3G networks and other WLAN technologies.

The rest of the thesis is organized as follows. Chapter 2 introduces WCDMA, WLAN (802.11) and location based services. Chapter 3 discusses radio propagation, handoff concept, traditional and emerging handoff algorithms, WCDMA handoff, WLAN handoff and the problems of vertical handoff. Chapter 4 presents the proposal of this thesis, including the idea of location-based vertical handoff, detailed architecture, handoff prediction/evaluation algorithms, signal detection algorithm, and multi-priority policy based handoff decision algorithm. Furthermore, evaluation results to validate the performance of the proposal on the number of handoff, battery consumption, handoff delay and drop call rate are presented. Chapter 5 draws concluding remarks and options for future work in this area.

Chapter 2

Technology Background

2.1 WCDMA And UMTS Radio Access

There are three primary standards for the third generation mobile networks: WCDMA, CDMA2000 and TD-SCDMA. They all adopt Code Division Multiple Access (CDMA), in which direct sequence spread spectrum is used. WCDMA was selected as the standard for Universal Mobile Telecommunication System (UMTS), as it is based on the Global System for Mobile Communication (GSM), the most widely used second generation mobile system.

Figure 9 shows the UMTS architecture UMTS is composed of two parts: core network (CS) and UMTS terrestrial radio access network (UTRAN), which communicates between User Equipment (UE) and CS. UTRAN consists of Radio Network Systems (RNS), which contains Radio Network Controller (RNC) and Node B. Each RNC controls one or more Node Bs and each Node B servers one or more cells. Node B implements WCDMA radio access physical channels including interleaving, channel coding, rate adaptation and spreading. RNC performs radio network control functions, such as: call establishment and release, handoff, power control, radio resource management, diversity combining, etc. To make connection with CS, UE needs to communicate through Uu interface with Node B, which in turn connects with RNC through Iu interface [23, 24].

According to the 3GPP standard, the radio interface is composed of three protocol layers: the physical layer (L1), the data link layer (L2) and the network layer (L3). Data link layer can be split into four sub layers: Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), and Broadcast/Multicast Control (BMC). Network layer and RLC can be divided into Control (C-) and User (U-) planes, while PDCP and BMC are only working on U-plane [24]. Figure 10 shows the radio interface architecture.

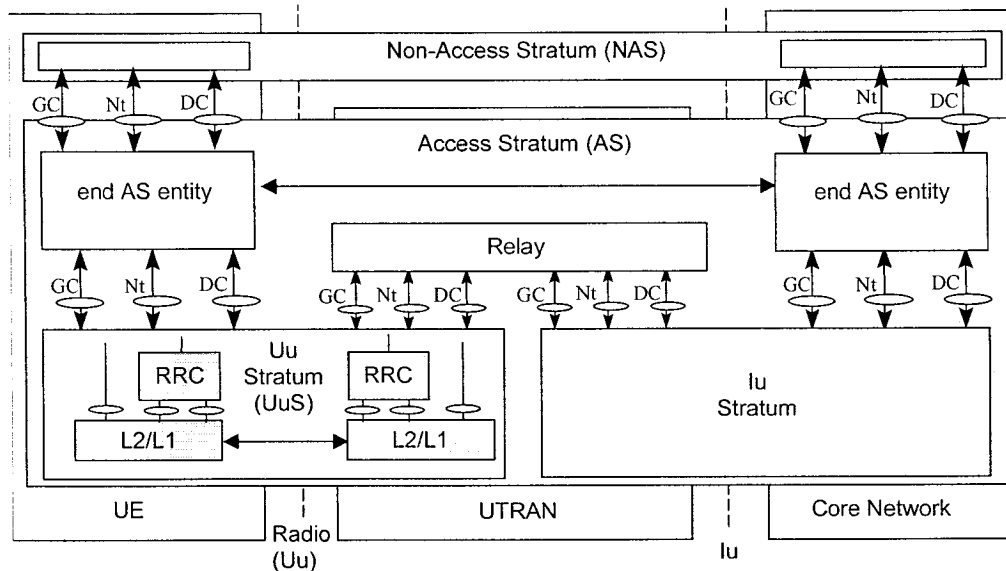


Figure 9. UMTS Architecture [24]

2.1.1 Physical Layer

The physical layer is connected to both MAC (L2) and RRC (Radio Resource Control L3) layers and is controlled by RRC. The physical layer provides MAC many kinds of transport channels, which is defined by how the data will transmit over the radio interface [25].

The WCDMA access scheme is Direct-Sequence Code Division Multiple Access (DS-CDMA) with approximately 5 MHz bandwidth [25], which means that all users share the same 5MHz spectrum and data is identified according to the channel code and cell-specific scrambling code. UTRAN has two duplex modes: Frequency Division Duplex (FDD) and Time Division Duplex (TDD). Convolutional coding and Turbo coding are all supported by these two modes. The modulation scheme is QPSK (8PSK is used for TDD with chip rate 1.28Mcps) [25].

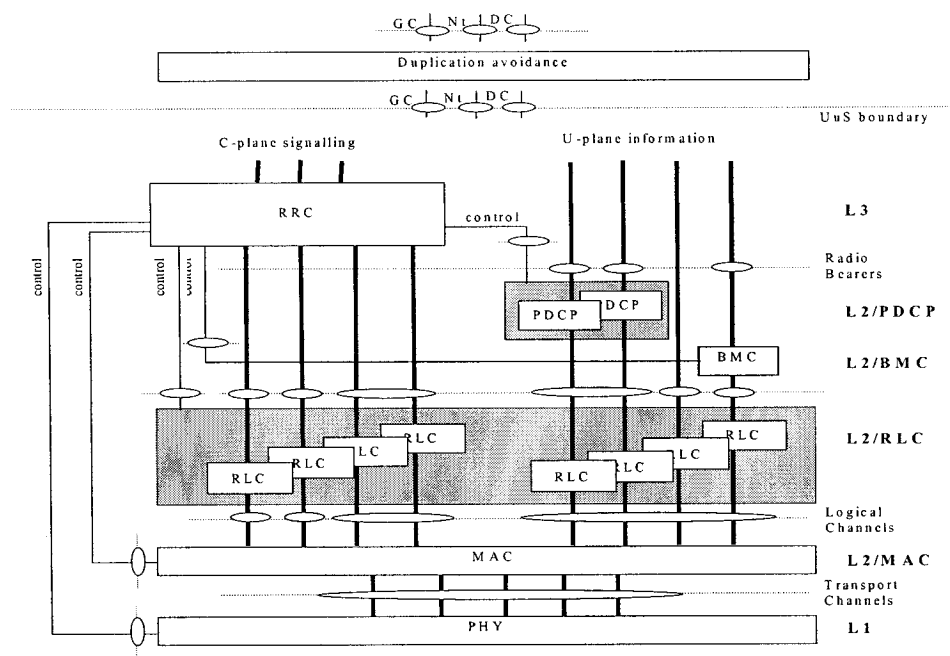


Figure 10. Radio Interface Protocol Architecture [24]

Measurement is one of the most important services provided by physical layer. Many network layer functions, such as handoff and power control, depend on measurement results from physical layer. The measurement of “SIR, UTRA carrier RSSI, GSM carrier RSSI, Transport channel BLER (block error rate), UE transmitter power, UE GPS Timing of Cell Frames for UE positioning and UE GPS code phase” [26] are mandatory in UE and the information of “Physical channel BER, Transport channel BER, Round Trip Time, SIR, UTRAN GPS Timing of Cell Frames for UE positioning, Cell Sync Burst SIR” [26] are required in Node B and will be reported to the RRC.

2. 1. 2 Media Access Control (MAC)

The MAC layer provides many kinds of transport channels between MAC and physical layer, including “Random Access Channel, Forward Access Channel, Downlink Shared Channel, and High Speed Downlink Shared Channel” [27]. Also, MAC will map transport channels to logical channels for the radio link control (RLC) sub-layer. Logical channels can be divided into two categories: control channel for control plane and traffic channel for traffic plane. Paging, broadcast and common control channel belong to control channel, while traffic channel include dedicated traffic, common traffic and MBMS point-to-multipoint traffic channel [27]. The MAC layer provides data

transmission, measurement reporting and reallocation of MAC parameters (radio resources) services for upper layer.

2.1.3 Radio Link Control (RLC)

RLC is composed of RLC entities, which have three modes: Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM). TM or UM entities can be configured into either a receiving RLC entity (receiver) or a transmitting RLC entity (sender), but not simultaneously. AM entity can perform the functions of a receiver and sender according to the context because it has both a receiving and transmitting side. The sender is responsible for sending RLC PDU. The receiver is responsible for receiving RLC PDU. They both can reside on either UE or UTRAN side. In TM the receiver can deliver the RLC Service Data Unit (SDU) to upper layers and the sender can receive it from upper layer through TM-SAP (Service Access Point) [28]. The UM does not provide a guaranteed PDU transmission to the destination entity, but the higher layer can check the sequence number field in the PDU structure to make sure the integrity of the data. “The UM is used when certain ACK and retransmissions signaling are part of the RRC procedure” [44]. Since no retransmission protocol deployed in the AM, PDU delivery cannot be guaranteed. Once data delivery is failed, the transmitting side will be notified and PDU will be retransmitted. In receiving side, PDUs will be stored in the buffer until a completed SDU is received. Then the PDUs will be reassembled and passed to the upper layer through AM-SAP. A successful acknowledgement or request for retransmission will be send back to the peer entity [28].

2.1.4 Packet Data Convergence Protocol (PDCP)

PDCP model exists only in the user plane and services the packet switched domain. The RB (Radio Bearers) for the PS domain RAB is associated with one PDCP entity, which can have one or two RLC entities. Every PDCP entity uses zero, one or several different header compression protocol types. PDCP only supports two header compression protocol types, RFC 2507 and 3095. PDCP contains compression methods, which are needed to gain spectral efficiency in the radio interface. PDCP protocol use RLC layer services in three different modes: AM-SAP (Data transfer is acknowledged), UM-SAP (Data transfer is unacknowledged) and TM-SAP (Data transfer in transparent mode) [29].

PDCP provides its services to the Non Access Stratum (NAS) at the UE or the relay at the Radio Network Controller (RNC).

2.1.5 Radio Resource Control Protocol (RRC)

RRC protocol entity exists on both the UE and UTRAN side. Figure 11 shows the RRC layer architecture. RRC protocol ensures that packets will not be lost or duplicated and the packets out of sequence can be restored after handoff or relocation. Also, RRC can coordinate the execution of resource control requests from the decisions made by the RRM algorithms [30].

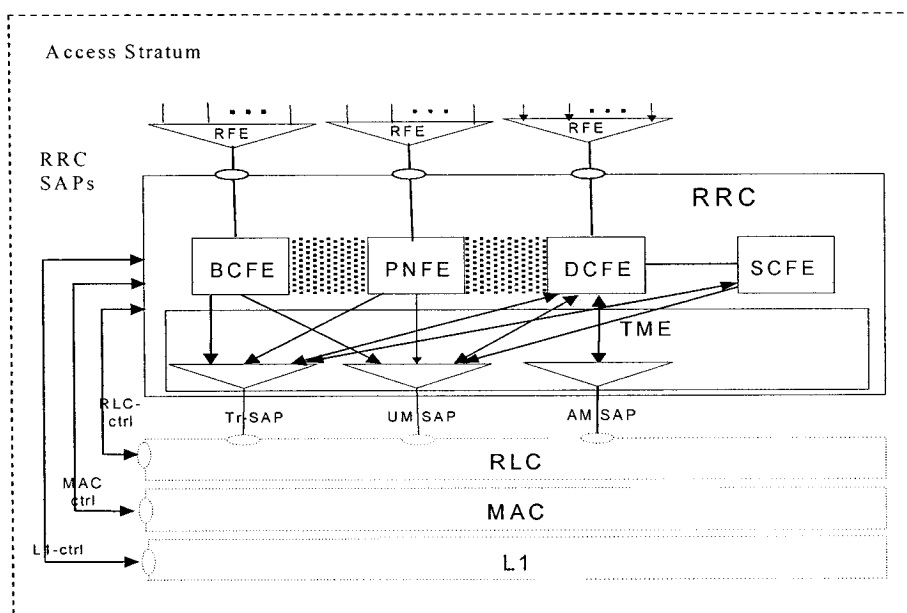


Figure 11. RRC Layer Architecture [30]

2.1.6 Radio Resource Management

Radio Resource Management (RRM) can exist on UE, Node B and RNC. RRM is a set of algorithms, which can manage and manipulate resource intelligently to guarantee the QoS, keep low blocking rate, map different service to physical channels efficiently, and optimize the overall system performance. RRM includes Power Control (PC), congestion control, Resource Manager (RM), and Handoff Control (HC) [51].

2.1.6.1 Power Control

Interference is a critical issue because all UEs are sharing the common frequency spectrum in WCDMA. To keep a good connection, we need to maintain the SIR above

the threshold for each UE. If the UE is at the boundary of cell, the probability that the SIR is below the threshold is much higher when the signals from other UEs are very strong. Interference control is especially important in the uplink direction because the system capacity can be adjusted by the required code power per each connection in the downlink direction. Power control (PC) is introduced to reduce interference and UE power consumption. PC function exists on all UTRAN entities and must be processed real-time because of the fast channel characteristics [31].

WCDMA power control is a closed-loop PC, which combines the inner and outer closed loop controls. Outer closed loop control is used to reduce the power consumption as low as possible, while keeping the communication quality above the requirement of bearer service quality. The uplink outer loop PC is aimed to set a target SIR in the Node B for inner loop PC. This target SIR is specific for different UE according to the estimated uplink quality in terms of Block Error Ratio or Bit Error Ratio. The downlink outer loop PC is used by the UE receiver to guarantee the required link quality set by RNC. Inner-loop PC adjusts the transmission powers dynamically based on the comparison of target SIR, which is set by out-loop PC, and measured SIR. Depending on SIR comparison results, Transmit Power Control (TPC) command is sent to transmitting entity in both Node B and UE [45].

2.1.6.2 Congestion Control

Power control cannot solve the CDMA-inherent interference problem if the system has reached a congestion status to some extent. Congestion control mechanism is supposed to be designed to deal with this situation, in which the QoS is hard to be guaranteed. Congestion control system in WCDMA is composed of admission control (AC), Packet Scheduler (PS) and Load Control (LC) [31].

The main function of AC is to check the current network load in this cell, estimate the effect to the existing connections if an extra radio access bearer (RAB) is established, because the introduction of new RBA will cause inter-cell interference. The network situation of adjacent cells also has to be taken into consideration, so AC can only be implemented in RNC, which has the information of surrounding cells. There are two kinds of AC: wide-band power-based AC and throughput-based AC. SIR has direct

relationship with cell load, power-based AC has a maximum value of noise rise caused by the new RBA, which can be set by radio network planning (RNP). Throughput-based AC uses the network load as the decision criteria. The RAB can only be accepted if the total load is below the RNP defined load threshold. AC is decided according to the current system load, interference measurements, service, expected QoS, and thresholds from network planning. If the connection is accepted, AC will set the proper parameters for this new RAB. AC has to control the real-time network traffic of the accepted radio bearers (RB), which may result in serious interference. For non-real-time traffic, AC together with PS will make optimum schedule for their transmitting time and bit rate [31][32].

The main responsibility of LC is to keep network load controllable and avoid overload. Overload situations seldom appears in RAN if AC and PS work well. However, if an overload occurs, the LC will immediately change the system load to the optimal value defined by the network planning. This function is called preventive load control. The AC and PS work together to implement the preventive load control and LC acts as a mediator. Measurements and estimations provided by AC and PS are used to update LC cell load status [31, 32].

PS is to determine the available radio interface resources and share these resources among non real time radio bearers. PS monitors the system loading and allocation status for non real time radio bearers. Also PS performs load control actions for the non-real-time radio bearers when necessary. PS is implemented on a cell basis. The cell radio resources are shared between non-controllable and best effort basis. PS in general can be based on power levels, throughputs, and spectrum efficiency. Total power from UL (RSSI) and DL measured by UE is sent via Iub to RCN using NBAP signaling protocol. Measurement reporting can be periodic or event triggered. Traffic volume and throughput are measured by RNC. AC and PS handle non-real-time bearer together. Load control algorithm is presented in [31].

PS is a combination of time division and code division scheduling. Time division scheduling allocates radio bearers for few high bit rate users, which has a short transmission time and therefore needs short data buffer. On the other hand code division

scheduling allocates low bit rate for high number of users depending on a load level. PS can work together with handoff control to control the air interface load and physical resources of the active set of each DCH users; work with LC and AC to solve the overload problem when total load is exceeding the target level [32].

2.1.6.3 Resource Management

The Resource Manager (RM) is responsible for reserving resources in terrestrial network, controlling the logical resources in Node B and RNC. The idea is to allocate physical radio resources requested by the RRC layer. RM has information about overall radio network configuration and connection UE states. RM is different from the other RRM function because it has connections only to the logical radio resources. The resource allocating process for each radio connection is more likely a reservation of proportion of the available radio resources according to the channel request from the RRC layer. First the RM gets information from the AC and PS. Then the RM informs the PS about network conditions. Finally scrambling codes in UL and the spreading codes in downlink direction are allocated. Codes can be changed for example during soft handoff or updating de-fragmented code tree [31].

2.2 WLAN Radio Access

2.2.1 System Architecture

Wireless Local Area Network (WLAN), which is based on IEEE 802.11 protocols, is another kind of widespread wireless technology. 802.11a defines a WLAN physical layer standard on 5GHz radio band with maximum link rate of 54Mbps per channel (8 channels totally) by using OFDM. 802.11b standard adopts DSSS on 2.4GHz radio band with maximum link rate of 11Mbps per channel (3 available channels). 802.11g defines a physical layer standard for the WLAN in 2.4GHz with 54Mbps per channel. 802.11g uses OFDM modulation, but is backward compatible with 802.11b.

The WLAN elements defined by 802.11 include terminal station (STA), access point (AP) and Portal. 802.11 architecture is illustrated in Figure 12. AP has both wireless and wired interfaces and works as a bridge between two kinds of networks.

Portal, an abstract concept of “translation bridge”, is always in the same physical entity as AP. The Basic Service Set (BSS) is a set of STAs that can communicate each other. BSS will work as an Ad Hoc network or called Independent BSS (IBSS) if no AP is within the BSS. STAs communicate on a peer-to-peer basis. Extended Service Set (ESS) is based on Distributed System (DS) infrastructure that interconnects BSS cells with APs. In ESS, all communication between STAs (within one BSS or in different BSS) or between a STA and a wired network go through AP [33].

The standard [34] separates the system into two parts: Media Access Control (MAC) of data link layer and Physical layer (PHY). Figure 13 indicates the 802.11 layer architecture. PHY is divided into two sub layers: Physical Medium Dependent sublayer (PMD) and Physical Layer Convergence Protocol sublayer (PLCP). Data link layer is divided into MAC and logic link layer (LLC) that contains the standard interface to network layer. Also, there are sublayer Management Entities on both PHY and MAC layers. In addition, an independent Station Management Entity is defined to provide status gathering, layer parameter control and system management functions (power control and channel selection). In this thesis 802.11b will be used as an example for detailed description of PHY, MAC layers and management entities.

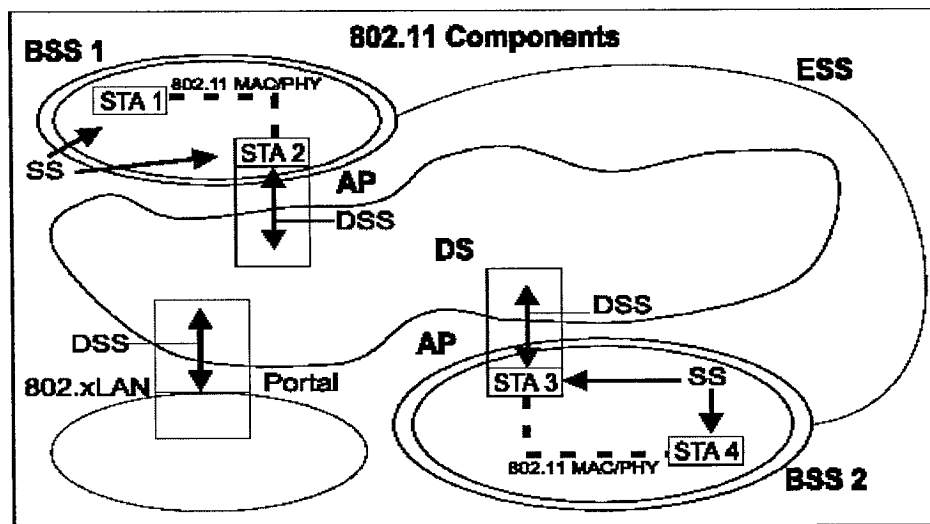


Figure 12. IEEE 802.11 Architecture [34]

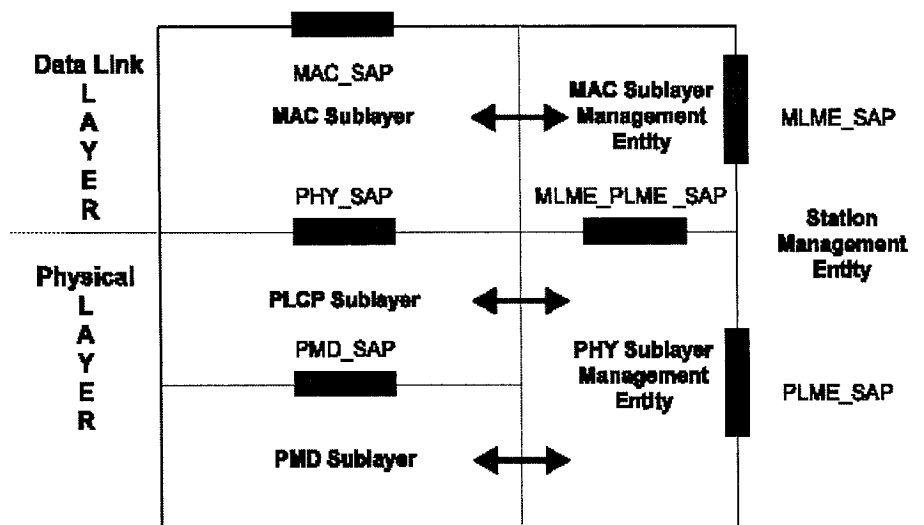


Figure 13. ISO/IEC Basic Reference Model Covered in 802.11 [34]

2.2.2 Physical Layer

The PHY layer can be split into two sublayers: the physical medium dependent (PMD) sublayer and the physical layer convergence procedure (PLCP) sublayer. The PMD defines how to use signal carrier and direct sequence spread spectrum (DSSS) to transmit and receive frames over wireless medium between STAs. 802.11b support two data rates: 5.5M and 11Mbps. The PLCP is responsible for exchanging each MAC PDU (MPDU) to a PLCP Service Data Unit (PSDU) that is in turn carried as PHY Protocol Data Units (PPDU). In this way, the MAC can be independent with PHY. In addition, a Physical Layer Management Entity (PLME) performs PHY management functions in conjunction with the MAC management entity [34].

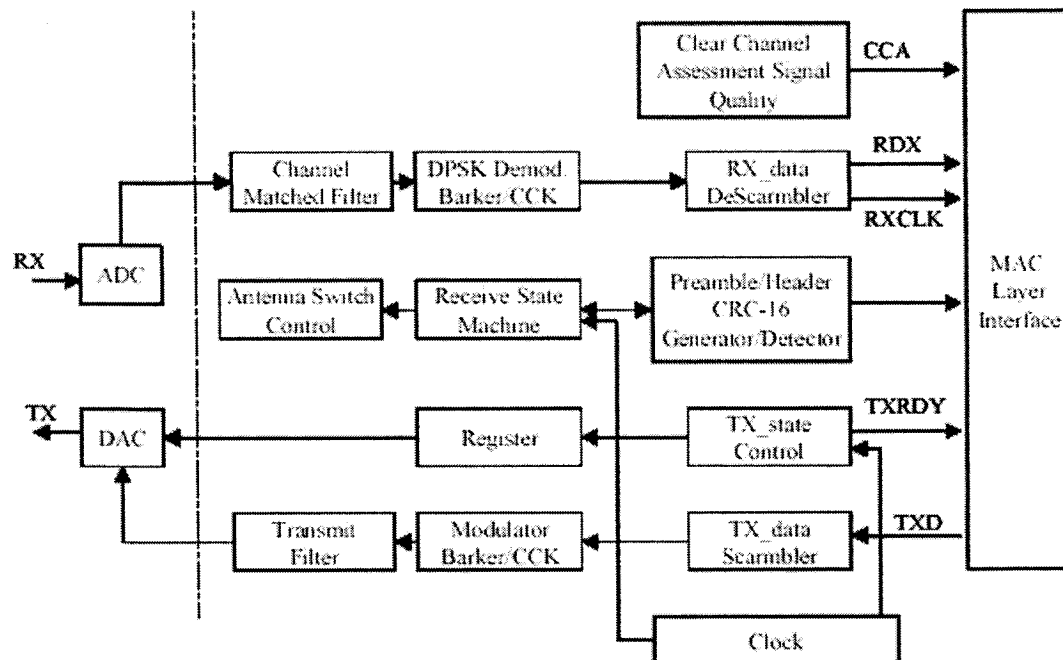


Figure 14 illustrates the functions of 802.11b PHY layer. 802.11b data is encoded with DSSS technology, in which data stream is multiplied by 64 CCK (Complementary Code Key) chipping sequence to achieve high bit rate. CCK is an M-ary Orthogonal Keying modulation where one of M unique (nearly orthogonal) signal codewords is chosen for transmission. To get a different transmission rate, a different modulation scheme is deployed [38].

The PPDU is composed of a PLCP preamble, PLCP header and MPDU, which will be transmitted to MAC layer. PLCP preamble contains Synchronization (Sync) and Start Frame Delimiter (SFD) fields. PLCP header includes signaling (SIGNAL), service (SERVICE), length (LENGTH) and CCITT CRC-16 fields, which are very important to transmit and receive the signal via RF medium. Both transmitting procedure issued from MAC and receiving procedure from STA to PLCP are defined in [34].

2.2.3 Medium Access Control (MAC)

MAC has interfaces with LLC and PHY layers. MAC layer provides three kinds of services: asynchronous data service, security service and MAC service data unit (MSDU)

ordering service. Asynchronous data service makes it possible to exchange MSDU between LLC entities. MAC can use PHY layer server to deliver a MSDU to the peer MAC entity, which in turn pass it to its LLC, on best-effort connectionless basis. Because there is no guarantee for the successful transportation, broadcast and multicast will suffer lower QoS than unicast MSDUs. Security service, which is limited between station-to-station data exchange, includes authentication service and WEP service. WEP can be regarded as an inner service within MAC because it is invisible to the LLC and any other layers above MAC. The WEP security services include confidentiality, authentication and access control together with layer management. MSDU Reordering is not happening unless it can improve the likelihood to deliver successfully. If the upper layer cannot tolerate the possible reordering, strictly ordered service class will be used [34]. Also, MAC protocol provides the functionality for reliable data delivery over the noisy and unpredictable wireless media, including channel allocation, protocol data unit addressing, frame formatting, error checking, fragmentation and reassembly [33].

The 802.11 model supports three kinds of frames: management, control and data frame. The management frames are used for STA association/disassociation, timing/synchronization, and authentication/de-authentication, while the control frames are used for handshaking, positive acknowledgment during CP. The data frames are used for the transmission of data during CP and CFP or they will be combined with polling and acknowledgments during CFP [44]. The 48 bits MAC address is used to identify a STA. MAC frame is composed with MAC header, frame body and frame check sequence (FCS). Header contains the information of frame control, duration, address and sequence control. The frame body has variable length consisting of 7 bytes optional Wired Equivalent Privacy (WEP) and data payload [34].

MAC can be divided into two sub-layers: the distributed coordination function (DCF) and the coordination function (PCF). Figure 15 shows the MAC layer architecture.

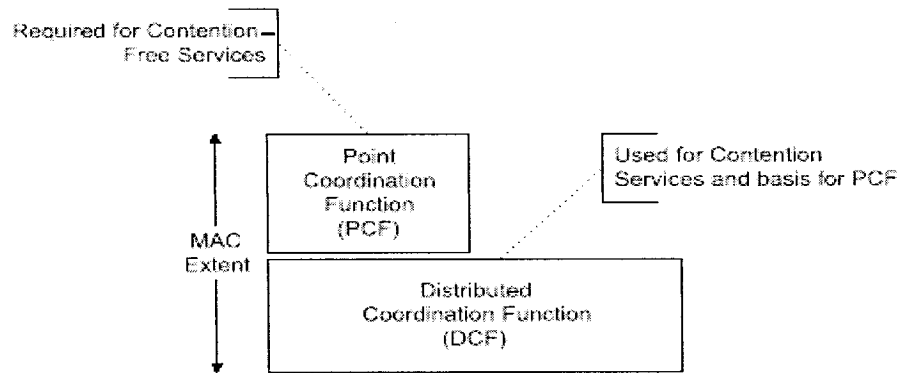


Figure 15. 802.11 MAC Architecture [34]

DCF is directly on top of physical layer and is the fundamental access method to support asynchronous data transfer. The fundamental access method of 802.11 is a DCF called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which should be implemented in all STAs because it is used by both IBSS and infrastructure network configurations. The CSMA/CA algorithm requires that between contiguous frame sequences a minimum specified duration T must exist. STA and AP must listen to the channel and detect it idle for this duration T before they can start data transmission. If a collision occurs, they have to defer some time before trying to transmit again. The reason why 802.11 does not use CSMA/CD (Collision Detection) is that STA is unable to listen to the channel for collision during transmitting. DCF supports contention services, which means that each STA with an MSDU queue ready for transmission must contend for access to the channel. Once the MSDU is transmitted, STA must reconnect the channel for the remaining frames. To minimize the collisions, STAs can exchange information in the header of Request to Send (RTS), Clear to Send (CTS) or data frame after knowing the medium is idle or after any deferrals (backoffs) prior to any new data transmission [34].

In addition, virtual and physical carrier-sense functions are used to determine the state of the medium. Only when both function indicate the medium is idle, it will be regarded as idle. Immediate positive acknowledge frame is used for all directed traffic. If no ACK is received, the sender will retransmit the packet. Priority to access the wireless medium is controlled by the inter-frame space (IFS) time intervals. Four IFSs are defined in the standard: short IFS (SIFS), PCF IFS (PIFS), DCF IFS (DIFS) and extended IFS

(EIFS). IFSs is independent with STA bit rate and IFS timings is defined as gaps on the medium and is fixed for each PHY according PHY attributes. The random backoff time is calculated by a pseudorandom integer drawn from a uniform distribution over the interval $[0, CW]$ (contention window (CW) is a value between aCW_{min} and aCW_{max}) multiplying a time slot determining by PHY characteristic [34]. In general, when a STA senses the channel is idle, it will wait for at least DIFS period and transmit a MPDU [34].

The IEEE 802.11 MAC also has an optional access mechanism called point coordination function (PCF), which is a centralized queuing method implemented on top of the DCF and is only used by infrastructure network configurations. PCF uses a point coordinator (PC), operating at the access point of the BSS, to determine which STA can transmit data at this time [34].

The PCF is connection-oriented and provides contention-free frame transfer. The transmission time can be divided into super-frames, which is composed of a Contention Free Period (CFP) and a Contention Period (CP). During the CFP, the PCF is used for accessing the medium, while the DCF is used during the CP. A CFP starts by a beacon frame and finishes with a CF-End frame transmitted by the AP. The beacon frame includes the information about the real duration of the CFP to update the NAV of the STAs as well as the network synchronization information. The AP polls each STA asking for pending frames to be transmitted. In case that the STA has any frames in queue it will transmit a frame. If the AP receives no response from a polled STA after waiting for a PIFS interval, it will poll the next STA [44].

The DCF and the PCF can coexist in the way that permits both to operate concurrently within the same BSS. When a PC is operating in a BSS, the two access methods alternate, with a contention-free period (CFP) followed by a contention period (CP) [34].

2.2.4 Layer Management

Both PHY and MAC have management entities: PHY sublayer management entity (PLME) and MAC sublayer management (MLME). A layer independent entity: station management entity (SME) should run on every STA to make MAC work correctly. Its main function is to gather layer-dependent information from various management entities

and set the value of layer-specific parameters. The management entities interact with each other via service access points (SAP), which may be SME-MLME SAP, SME-PLME SAP or MLME-PLME SAP. The management information of each layer is stored as the corresponding management information base (MIB) [34]. The MIB is composed of “managed object, attributes, actions, and notifications required to manage a station” [34].

The interfaces supported by PLME include “PLME-GET, PLME-SET, PLME-RESET, PLME-CHARACTERISTICS, PLME-TXTIME, PLME-CHARACTERISTICS, PLME-DSSSTESTMODE and PLME-DSSSTESTOUTPUT” primitives [34]. The MAC Management Layer is responsible for “synchronization, power management, association/reassociation and MIB definition” [34].

2.3 Location Based Service

As location based services (LCS) get more and more popular, they have pushed 3GPP to standardize these services for UTRAN. 3GPP defined four kinds of LCS clients: “emergency service client, lawful intercept client, Public Land Mobile Network (PLMN) operator client and Value-Added Service client” [39]. Location aided vertical handoff between 3G and WLAN belongs to PLMN operator client. Also, the standard categorized the LCS functions into four groups: “Position Radio Coordination Function (PRCF), Position Calculation Function (PCF), Position Signal Measurement Function (PSMF) and Position Radio Resource Management (PRRM)” [39]. Location Information consists of Geographic Location, Quality of Service information and Velocity, which is the combination of speed and moving direction of UE [39].

2.3.1 3GPP LCS Architecture

3GPP UTRAN Positioning architecture is indicated in Figure 16. Location Measurement Unit (LMU) can be either associated with Node B or be a stand-alone entity connecting with Node B via Uu interface. The Serving RNC (SRNC) is the entity to implement LCS functionality, including UE position calculation, estimation of accuracy, database access, making co-ordinate translation and communication with CN across Iu interface. SRNC can work either in RNC centric mode or in Stand-Alone Serving Mobile Location Center

mode. UE will transmit signals for uplink based positioning measurement and also make measurement on the downlink signal. In general, UE position procedure in UTRAN starts from CN. CN sends request to SRNC through Iu interface. Then SRNC sends measurement request to LMU, which collects the measurement information and sends it to SRNC, where location information is calculated and is transmitted back to CN [39].

2.3.2 3GPP Positioning Method

The positioning methods supported by UTRAN include: *cell ID based methods*, *Observed Time Difference Of Arrival (OTDOA)*, *network-assisted GPS methods* and *Uplink – Time Difference Of Arrival (U-TDOA)*. Each method exhibits some attributes that make it suitable for some environment and applications. A hybrid approach is recommended to get high positioning accuracy [39].

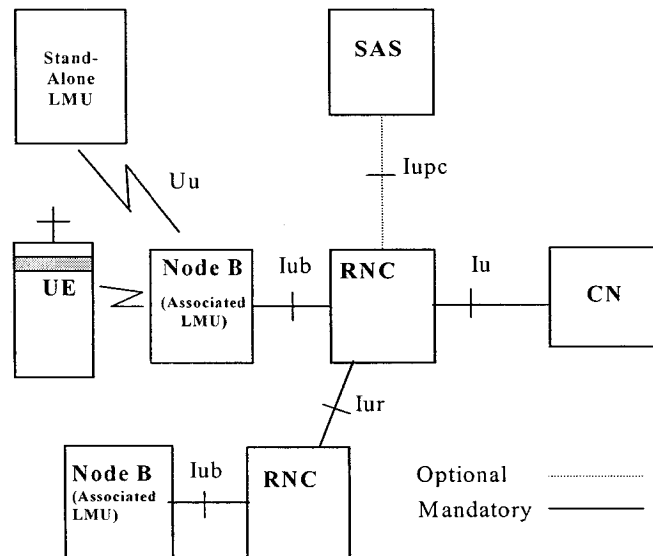


Figure 16. Architecture of UE Positioning in UTRAN [39]

In the *cell-ID based method*, UE position is decided by its serving Node B. The information can be obtained by location area update, cell update, routing update or paging. The estimated position can be a specific location of the cell. The accuracy depends on the cell size which is from 2km to 20km in diameter. For pico cells, the accuracy is 150 meters. If the position information can be combined with other factors, such as the signal RTT for FDD mode or Receiver timing deviation measurement, UE timing Advance (TA) or Signal Strength together, the accuracy will be increased dramatically [39].

OTDOA is E-OTD version on WCDMA system, while E-OTD is used on GSM and GPRS network. The OTDOA location services technique estimates the UE position by comparing the receiving time of WCDMA frames at least from three different Node Bs. If the number of Node B is not large or it is a linear network in this area, the accuracy will be very poor, because WCDMA is optimized for low power and the efficient use of bandwidth. The ability to see and use multiple Node B station is severely limited, so overall OTDOA performance is worse than average E-OTD [39].

GPS is a satellite navigation system funded by US Department of Defense. The GPS receiver in the UE measures the time required to transmit from one point to another. If receiver can calculate the distance from four satellites, UE can get the accurate position on earth. But it requires the signal from satellite pretty strong to get the accurate time information. Network-assisted GPS overcome this limitation by reducing the UE start-up and acquisition times, increasing the UE GPA sensitivity and consuming less power than stand-alone GPS. “The Network-assisted GPS methods rely on signaling between UE GPS receivers (possibly with reduced complexity) and a continuously operating GPS reference receiver network, which has clear sky visibility of the same GPS constellation as the assisted UEs. GPS reference receivers may be connected to the UTRAN to enable derivation of UE assistance signals” [39]. The typical accuracy of GPS is 10m. To increase the accuracy of position estimation, DGPS is used, in which biases in the pseudorange measurements is provided to the UE. Ming-Hsing Chiu in [41] said that the accuracy at 3-5m can be achieved. However, GPS is inefficient for indoor use or in urban areas where high buildings shield the satellite signals.

“The *U-TDOA positioning method* is based on network measurements of the Time Of arrival (TOA) of a known signal sent from the UE and received at four or more LMUs. The method requires LMUs in the geographic vicinity of the UE to be positioned to accurately measure the TOA of the bursts. Since the geographical coordinates of the measurement units are known, the UE position can be calculated via hyperbolic trilateration. This method will work with existing UE without any modification” [39]. In order to achieve the most accurate estimate of the UE’s position, more hyperbolas must be calculated. The hyperbolas need to cooperate with more U-TDOA, which are capable to use LMUs in the calculation. U-TDOA works exceptional well in indoor and urban

area. However, the performance is not good in rural area because the number of LMU is limited. As the number of LMU increased, the accuracy of U-TDOA will be increased. Normally the accuracy of U-TDOA is 35-50 meters.

The *network-assisted GPS* requires the UE having GPS receiver in it. Considering the cost and battery consumption, OTDOA and U-TDOA are good solutions, which are now being widely adopted by vendors. Many companies, such as CAMBRIDGE Positioning Systems Ltd (CPS), have delivered improved performance for 3GPP U-TDOA/OTDOA standard with sub-20 meter accuracy. In 3G networks, if hybrid positioning methods, such as U-TDOA and Network-assisted GPS combined, we can get more accurate location information for wider area.

2.3.3 WLAN Positioning Method

IBM Research Lab reports in 2004 that its WLAN-based position system can achieve 2m accuracy with 90% probability for static position determination. For mobile devices, a 5m accuracy can be achieved for 90% probability [42]. The experiment results in [43] showed that positioning accuracy of 1-3m can be achieved and they also claimed that they could provide 0.1m accuracy in idealized situation.

There are many positioning products for 802.11 wireless networks. For example, Ekahau's positioning technology is based on "signal strength calibration and fingerprinting, which ensures the highest possible granularity" [54]. It is said that Ekahau Positioning Engine 3.1"(EPE) is capable of pinpointing Ekahau T201 Wi-Fi Tags, laptops, PDAs and other Wi-Fi enabled devices, with floor-, room- and door-level accuracy" [54]. The position accuracy is within 1m [54].

As it is known, the accuracy of 3G positioning in indoor and urban environment is around 20m right now. It is not correct enough to navigate an accurate vertical handoff, but it provides the basic position information in wide coverage. If the 3G positioning information is combined with WLAN positioning information, we can get a good vertical handoff method.

Chapter 3

Handoff Algorithms

3.1 Cellular Basics

The wireless radio channel is not a reliable medium for high-speed communication because it is affected by noises and interferences that are changing in unpredictable ways due to the mobility of UE and the environment. The variation of receiving signal power is caused by three reasons: path loss, shadowing and multi-path fading. “Path loss is caused by dissipation of the power radiated by the transmitter as well as effects of the propagation channel. Path loss models generally assume that path loss is the same at a given transmit-receive distance. Shadowing is caused by obstacles between the transmitter and receiver that absorb power. The signal is blocked when the obstacle absorbs all the power” [46]. The reflection property of radio signal makes a single pulse being received as a pulse train from different paths with different time delay, phase and strength. Figure 17 is the ratio of the received-transmitted power in dB versus log-distance for these three combined fading effects.

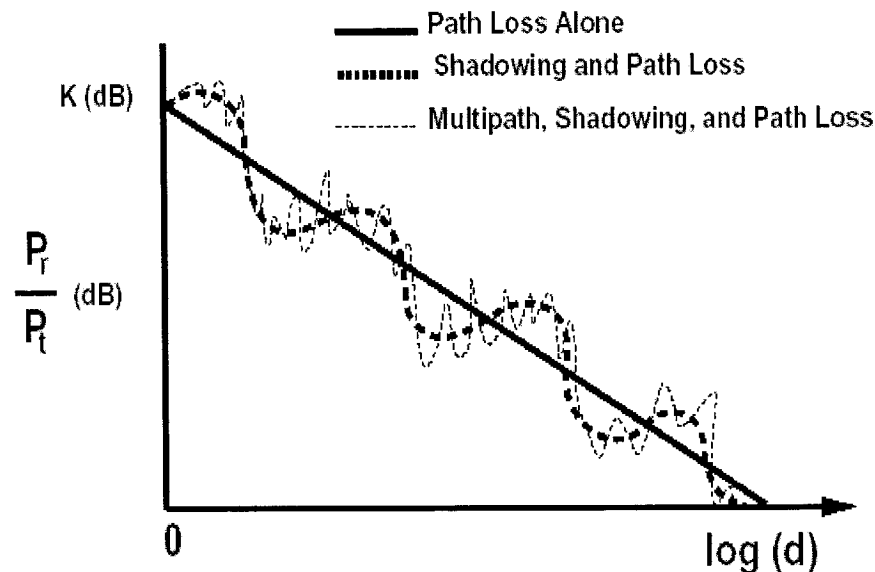


Figure 17. Path Loss, Shadowing and Multi-path versus Distance [46]

The cellular system is composed of non-overlapping cells assigned with different frequencies, timeslots or codes. For FDMA/TDMA, cells with same frequency or timeslot are spaced only far enough apart to avoid mutual interference. The codes are reused for every cell in WCDMA. In each cell the central transmitter is connected with a Node B and RNC, which acts as a central controller and performs channel allocation, power control, and handoff, etc. RNC will initiate a handoff if the received signal strength is too weak due to path loss, shadowing, and multi-path fading. The basic idea of cellular system is frequency reuse, which increases the spectral efficiency. The spectral efficiency per unit area is increasing by shrinking the size of cell, since more UE can be accommodated in this area. Optimal cell organization for UMTS radio coverage is a hierarchical cell structure (HCS) that introduces macro, micro and pico cells. Large macro cells guarantee a continuous coverage for fast moving mobile terminals and small pico-micro cells enlarges spectrum efficiency for high capacity in hot spot areas. The maximum bit rate for macro cells is likely to be 384 kbps and 2 Mbps for pico cells. However, WLAN is designed to function in pico cell area that introduces two traffic models, Ad Hoc and personal area network (PAN). Most of the traffic is exchanged within the pico cell. Therefore, hot-spot design applies to this nonhierarchical cell structure. WCDMA deployment scenarios use HCS in which cells in different horizontal layers have different carriers. A smaller cell with another carrier can be introduced below large umbrella cells. This method is more effective than increasing Node B transmission strength and can be used especially in hot-spot areas in order to gain the capacity necessary for highly loaded cells [46].

The channels for WCDMA are semi-orthogonal due to the spreading code properties. Although these codes allow channel reuse in every cell, they also introduce interferences from all users within the same cell (intracell interference) as well as from users in other cells (intercell interference). To compensate for the near-far problem of the intracell interferers, most CDMA systems use power control. When the mobile terminal is close to the boundary of cell, the received signal power will be very weak. The power control will boost up the transmitting power, which greatly increases the interference to the adjacent cells. The huge number of interference makes it pretty complex to analyze

the performance of the CDMA system, which “depends very heavily on the propagation model, cell size, mobility models, and other system parameters” [46].

3.2 Handoff

“Handoff is the process of changing the channel (frequency, time slot, spreading code, or combination of them) associated with the current connection while a call is in progress” [48]. Handoff is triggered by either UE crossing the cell boundary or the deterioration of the signal in the current channel. Handoff can be divided into two categories: *hard handoff* and *soft handoff*. Hard handoff is also called “break before make” while soft handoff is called “make before break” [47]. In hard handoff, the current serving resource is released before the new link is established; while in soft handoff, during the period of handoff, UE is connected with several Node Bs before choosing a destination with strong signal or high quality signal. WCDMA is using soft handoff. Another classification of handoff is based on where the decision control is located. If it is located in network entity (such as cellular voice system), it is called network controlled handoff (MCHO); while, it is called mobile controlled handoff (NCHO) if the decision is made by UE. The handoff in GPRS is mobile assisted handoff (MAHO) because the network entity needs the information from UE to make a decision [47].

The process of handoff can be broken down to five components: measurement, processing, deciding, executing and feedback [46]. The measurements are made in UE or LMU. Many kinds of measurements are used for a handoff decision. Together with other measurements, the uplink signal power is used by most of the first generation cellular systems like AMPS, and the second generation system like GSM, IS-54. Also, uplink bit error rate (BER), carrier-to-interference ratio (CIR), signal-to-interference ratio (SIR), block error rate (BLER), the path loss, location (distance) measure and maximum Doppler frequency, etc. are used for handoff decision. Measurements can be processed to generate useful input to the handoff decision algorithm. Most of the schemes do not perform much processing. The decision process is a key component to answer when and where to handoff. The execution phase deals with how to make handoff and involves with network architecture and protocol. After the handoff is done, the system is supposed to evaluate this handoff and prepare to make improvement on future handoffs [47].

Every handoff will cost network resource in terms of over-the-air signaling, network signaling, database querying, channel reallocation and network reconfiguration because the handoff process involves physical layer, data link layer and network layer for both UE and Node B (access point). The interface signaling and control signaling will consume much radio bandwidth and takes much time to make communications between both sides. Database accesses for registration and authentication also contribute to the handoff cost. Network configurations, such as setting up and tearing down of links between network entity and bridging, are necessary for UE to access the new base station and stopping access the old one [49]. Vertical handoff has higher network consumption and longer delay because the handoff process between two different wireless networks is much more complex than the traditional handoff.

Efficient handoffs are becoming more and more important for wireless communications. In order to increase the system capability and frequency reuse ability, smaller cells, such as micro-cells or pico-cells (WLAN) are widely used especially in urban and indoor environments. Smaller cells indicate that UE has to make movements between cells frequently; therefore, more frequent handoffs are required [49]. As mentioned in Chapter One, 3G networks and WLANs are complimentary. In order to get better service, vertical handoff is supposed to be made at the correct time and location. Unfortunately, each time when a handoff is attempted, the call may be dropped or the data transmission may be terminated. Complex vertical handoff will result in much higher failure rates. Given the increasing number of handoff and much complicated vertical handoff process, the per-handoff accuracy and efficiency of the handoff algorithms must be increased. Also, handoffs will bring some intolerable effect on the quality of service, such as brief loss of voice and delayed packets transmission [49]. In addition, unnecessary vertical handoffs will greatly increase the signaling load and seriously decrease the network performance.

In summary, we expect an efficient handoff algorithm to perform the only necessary handoffs with low call drop rate in correct time and location.

3.3 Handoff algorithms

3.3.1 Strength Based Algorithm

The most widely used traditional handoff algorithm is the strength based algorithms, of which the simplest one is the relative signal strength algorithm. UE always chooses the Node B with the stronger signal strength, (i.e. choose B_{new} , if $P_{new} > P_{old}$). The disadvantage is that it will introduce many unnecessary handoffs due to shadowing and Rayleigh fading fluctuation. This is called the ping-pong effect. A variation of the basic relative signal strength algorithm is to incorporate hysteresis. A handoff is made if RSS from new Node B is greater than RSS from current serving Node B by hysteresis. Hysteresis greatly reduces the ping-pong effect and unnecessary handoff. On the other hand, it makes the handoff procedure a little bit delayed, and the delay period is increased with hysteresis getting larger. It is obvious that there is a trade-off between average delay and the number of unnecessary handoffs. To get balance between proper handoff number and handoff delay, appropriate hysteresis and signal strength averaging methods should be chosen. Another variation of relative signal strength algorithm is using Dwell Timer. A timer is started when $P_{new} > P_{old}$. If the condition continues to be true until the timer is expired, a handoff will be launched. Soft handoff can avoid the ping-pong effect because the handoff algorithm does not make a quick decision like hard handoff. During the transition period, UE will make connections with multi-Node Bs simultaneously before choosing the most suitable handoff destination. Also, taking advantage of the diversity, the RSS can be stronger during this period. Unfortunately, soft handoff is not suitable for vertical handoff between two different wireless technologies with different frequency, modulation and coding scheme.

Another strength based algorithm is the absolute signal strength algorithm. A handoff will be launched when the RSS drops below the threshold level, which could be varied according to path loss slope L of the RSS and the level crossing rate (LCR) of the RSS. If either L or LCR is high, it means UE is moving towards the boundary of cell fast, so the threshold should be higher, otherwise, the threshold value should be lower. Velocity and L can be used to decide the threshold dynamically to avoid the unnecessary

handoff and keep handoff successfully. In some cases, this algorithm does not work well. For example, when the high RSS is resulted from high interference, a handoff is expected but will not happen, while sometimes the RSS is low but the voice quality is good enough, a handoff will be made unnecessarily. A variation of absolute signal strength algorithm is using two thresholds $L1$ and $L2$ ($L1 > L2$). If the signal strength is below $L1$ but greater than $L2$, the handoff is requested and assessed. When the RSS from new candidate cell is stronger or the RSS from current cell is less than $L2$, the handoff will be performed [49].

In some cellular systems, absolute signal strength algorithm and relative signal strength algorithm are combined. To trigger the handoff, two conditions must be satisfied: the average RSS from current cell is below an absolute threshold R and the average RSS from candidate cell is greater than the RSS from serving cell by hysteresis H . Also, such conditions are supposed to be satisfied for a period of time T . The first condition avoids the handoffs when the current cell can still provide good service, while the hysteresis and time restriction will decrease ping-pong effect. But it is obvious that the number of unnecessary handoffs will increase if the T and H are smaller, while if T and H increase, the number of unnecessary handoff will decrease but the delay will be increasing. The trade-off still exists [50].

3.3.2 Other Handoff Algorithms

Distance based algorithms connect the UE with the nearest Node B. They use the propagation time delay to get relative distance information. Although it has high efficiency compared to the RSS based algorithm, the inaccurate distance information and complex radio propagation property make it impractical.

Besides signal strength, SIR, BER are other important factors to measure the signal quality. SIR based algorithm is also widely deployed. This algorithm makes a handoff when the SIR in current serving BS drops below a threshold and the SIR of another candidate cell is sufficient. Hysteresis and time period are also used in the same way as the signal strength based algorithm. Because the low SIR means high interference or low carrier power, SIR reflects the real signal quality for most situations in which handoff is desirable. However, SIR is still high at the cell boundary in some system such as AMPS and GSM, which prevents the necessary handoff [50].

Another algorithm is the RSS and BER based algorithm. This algorithm combines the signal strength and signal quality as the measurements for handoff decision. Many cellular systems use multi-measurement to increase the accuracy of handoff. In GSM system, three measurements: received signal strength, received signal quality in term of chip error rate, absolute distance between base station and user are used to make a handoff decision. In this algorithm, RSS threshold, BER threshold and RSS hysteresis are used. The basic principle is the same with the traditional RSS based algorithm, but multi-factors have been considered [50].

In addition, velocity adaptive based, direction biased based, minimum power based algorithms have been proposed. However, the ping-pong effect and the issue of trade-off between unnecessary handoff and handoff delay are still not solved perfectly [50].

3.3.3 Emerging Handoff Algorithms

The emerging handoff algorithms include dynamic programming based, pattern recognition prediction based, Fuzzy logic and neural network based algorithms. Dynamic programming introduces a systematic method to do optimization. Handoff is regarded as a reward/cost or obtaining a tradeoff between the expected handoff number and number of service failure optimization problem. Optimal model is established and evaluation methods are defined, but the scenarios used for the simulation are simple and ideal. Wong [47] uses a template-based pattern recognition to initialize handoff whenever a UE is at or near the pre-selected locations. This algorithm needs a long time pre-study process and also only a simple canonical problem is examined. For a practical cellular system, the situation is much complex. Tripathi proposes a fuzzy logic and neural network based handoff algorithm [50]. These emerging handoff algorithms have not been accepted by the second generation and third generation mobile systems.

3.4 WCDMA Handoff

The WCDMA handoffs can be divided into two categories: inter-frequency handoff and intra-frequency handoff. If different carriers are allocated to handoff cells (such as cells

between GPRS and WCDMA, WLAN and WCDMA), inter-frequency handoff, which is definitely a hard handoff, will be launched. On the other hand, intra-frequency handoff can be hard handoff, soft handoff and softer handoff.

The overall handoff process is implemented in UE and RNC. UE is responsible for measuring the network parameters; while RNC is responsible for defining the type of measurement. UE measures the downlink signal strength and quality from serving cell and candidate cells, and then sends them to RNC. RNC also measures the uplink signal from serving Node B for the UE. RNC uses these measurements, defined threshold, hysteresis and handoff strategy to make the handoff decision. The measurements are based on E_b/I_o (the received energy per chip divided by the power density in the band). The UE constantly monitors the CPICH E_b/I_o of the cells defined by the neighboring list. UE sends an event triggered measurement report when the reporting criterion is fulfilled. Reporting of measurement results can be either event-triggered or periodic. The cause of handoff can be uplink signal parameters (e.g. BER, RSCP), downlink signal measurement (e.g. BLER, CPICH RSCP, CPICH E_c/N_0 , pathloss), distance, change of service and traffic load, etc. [51].

3.4.1 Hard Handoff

Hard handoff procedure is described in [30], received measurement report and load control can be used for decision. In WCDMA, hard handoff is used when radio frequency band of the connection between UE and UTRAN is changed or when no network support of macro diversity exists during cells changing. Also, when UE is roaming into a new cell of UMTS and soft and softer handoff are not available, hard handoff will be chosen. Another important application of hard handoff is inter-system handoff, such as WCDMA/GSM or WCDMA/GPRS, which will be discussed soon.

3.4.2 Soft and Softer Handoff

Soft and softer handoffs (SHO) are specific for CDMA system, which are implemented in the UMTS system and are the most characteristic features of the WCDMA access mechanisms. Objectives of soft and softer handoff are, "Optimum fast closed loop PC as the terminal is always linked with the strongest cells; Seamless handoff without disconnection of the radio access bearer; Diversity gain by combining the received

signals from different cells; Enabling better coverage and less transmission power” [51]. During soft handoff UE is simultaneously controlled by two or more cells belonging to different Node Bs under the same or different RNCs. Combining two radio links from two Node Bs is performed using Macro diversity combining, which re-connect the data streams in radio links over number of Node Bs. For softer handoff, UE has established connections with at least two cells controlled by the same Node B. Micro diversity function is also deployed to combine these two radio links [51].

Decision algorithm of SHO is located in RNC. All RRM functions participate in the SHO process. First, AC needed for admission decision for RT RB and queuing in case of congestion. Second, RM allocated and releases the DL spreading code, and activates radio link for new handoff branch. Third, downlink load information is to be updated by LC when new RT RB is admitted. Fourth, PS priorities are added the handoff branch in the case of NRT [44].

SHO is mobile assisted handoff (MAHO). UE continuously measures signal from cells defined in Monitored Set and report measurement results to SRNC. Once UE detects a new Node B in another RNC area, SRNC will check if this Node B fulfill soft handoff requirement. If so, radio link and bearer will be established and SRNC will update Active Set [44]. “Active Set is defined as the set of radio links simultaneously involved in the communication between the UE and UTRAN (i.e., the UTRA cells currently assigning a downlink DPCH to the UE constitute the active set)” [51]. Soft Handoff function will use signal measurements to evaluate which Node B should be added, removed from or replaced in the Active Set and then perform "Active Set Update" procedure to maintain the Active Set [51].

Figure 18 shows the soft handoff algorithm. Any of the measurements quantities listed in [30] can be considered. In this graph: “

- AS_Th: Threshold for macro diversity (reporting range);
- AS_Th_Hyst: Hysteresis for the above threshold;
- AS_Rep_Hyst: Replacement Hysteresis;
- ΔT : Time to Trigger;

- AS_Max_Size: Maximum size of Active Set.

As described in the figure above:

- If Meas_Sign is below $(\text{Best_Ss} - \text{As_Th} - \text{As_Th_Hyst})$ for a period of ΔT remove Worst cell in the Active Set.
- If Meas_Sign is greater than $(\text{Best_Ss} - \text{As_Th} + \text{As_Th_Hyst})$ for a period of ΔT and the Active Set is not full add Best cell outside the Active Set in the Active Set.
- If Active Set is full and Best_Cand_Ss is greater than $(\text{Worst_Old_Ss} + \text{As_Rep_Hyst})$ for a period of ΔT add Best cell outside Active Set and Remove Worst cell in the Active Set.

Where:

- Best_Ss :the best measured cell present in the Active Set;
- Worst_Old_Ss: the worst measured cell present in the Active Set;
- Best_Cand_Set: the best measured cell present in the monitored set.
- Meas_Sign :the measured and filtered quantity” [51].

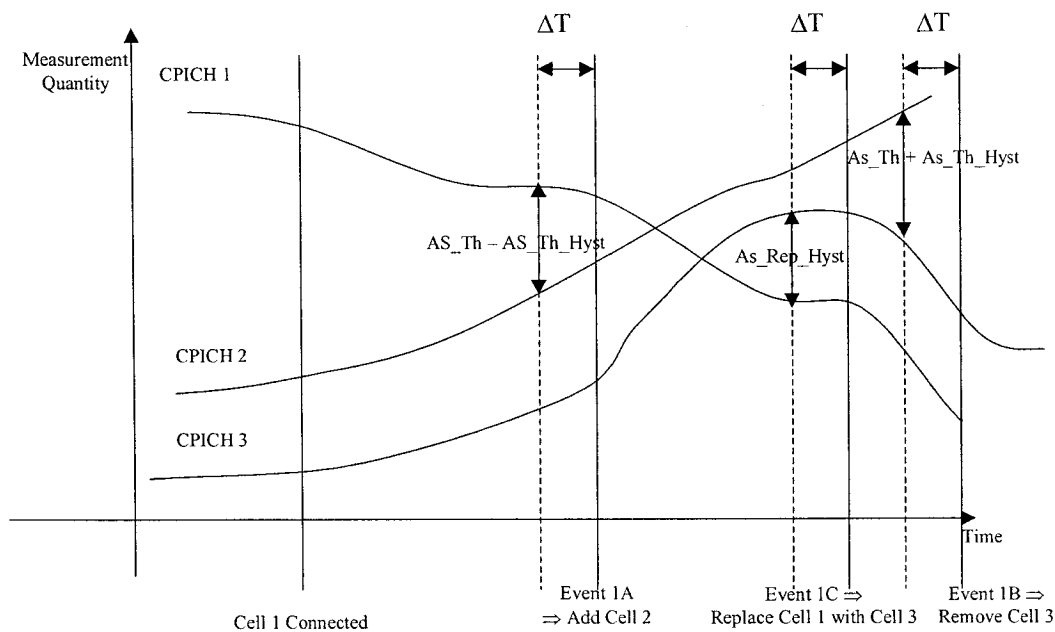


Figure 18. WCDMA Soft Handoff Algorithm [51]

3.4.3 Intersystem Handoff

Intersystem handoff (ISHO) is a hard handoff between different radio access technologies (RAT). Handoff between UTRAN and GSM is discussed in [51]. ISHO is often used to

balance network load or let UE access to certain service that is available in current connected RAT. Although ISHO is Network Evaluated handoff and handoff decision algorithm is running in RAN, UE must have multi-interfaces to support ISHO.

Now let us introduce ISHO between UTRAN and GSM. In the TDD mode, UE can measure the signal during idle time slots or the specifically assigned downlink. In the FDD mode, UE can make measurements by using idle time slots created by downlink compressed mode. Inter-system information exchanging is necessary to let UTRAN notify UE the GSM frequency in this area. To make a handoff from GSM to UTRAN, predefined radio configuration and other RRC information, such as security information and UE radio capability, are required. By downloading predefined radio configuration, which is composed of radio bearer and transport channel parameters, only additional parameters are need to be transmitted during handoff. UE can store up to 16 different predefined radio configurations for different services: speech, circuit switched data, and so on. Furthermore, it is optional for a network to decide whether to use pre-configuration or not; the handoff procedure also supports transferring all parameters and the use of default configurations. Security information includes the initialization parameters for ciphering, integrity protection and ciphering algorithm. When RRC radio configuration parameters are included in the handoff (GSM to UTRAN) message, UTRAN should consider the capabilities of UE. Therefore, RNC should get the information about UE radio capability before the handoff from the GSM to UTRAN [51].

The handoff from GSM to UTRAN includes the following stages:

- UE Downloads predefined configuration information broadcasted by UTRAN
- BSS queries UE capability, security and predefined configuration information
- The BSS configures the UTRA measurements, including the concerned thresholds and the reporting parameters.
- The predefined configuration status information is included in the UTRAN CLASSMARK CHANGE message, which indicates if the UE have the required predefined configuration stored. If not, the BSS might use full signaling or one of the default configurations for the handoff from GSM to UTRAN process. BSS

will initiate a handoff when the BSS has made a handoff decision triggered by the reception of a measurement report [51].

- Then, the CN will request resources from target RNC by sending a Relocation request message. This message should include UE capability, security information that is obtained by the BSS previously, handoff service type and the predefined configuration status information. The target RNC will select the predefined configuration for the UE according to the indication of service type. The main reason to include the predefined configuration status is that “when selecting the predefined configuration to be indicated within the handoff to UTRAN command message, the target RNC should know if the UE has downloaded all predefined configurations or only a subset” [51].

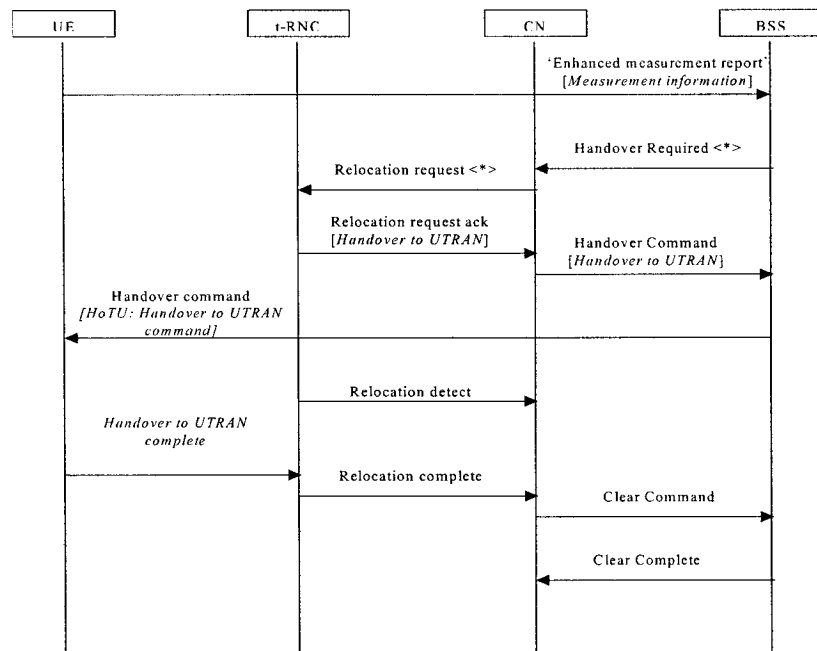


Figure 19. Handoff from GSM to UTRAN [51]

3.5 WLAN Handoff

Roaming is not defined in the 802.11 standard. STA simply detects the signals and associates the AP with strongest signals. The scanning process will start when the current

Radio Signal Strength becomes weak. Passive scanning process can listen to available APs because AP will broadcast a beacon signal in every short time period, which includes time stamp for synchronization, traffic indication map and supported data rate, etc information. However, active scanning process will send out a probe request. After receiving the response from APs, STA will compare the receiving beacon strength with current connection and select the candidate AP with strongest signal. Then STA will send a re-association request to this new AP. When the new AP accepts the request, the AP will send re-association message to STA and indicate the re-association to the DS as well. The new connection will be established after STA gets the response from AP. Figure 20 shows a handoff scenario [44].

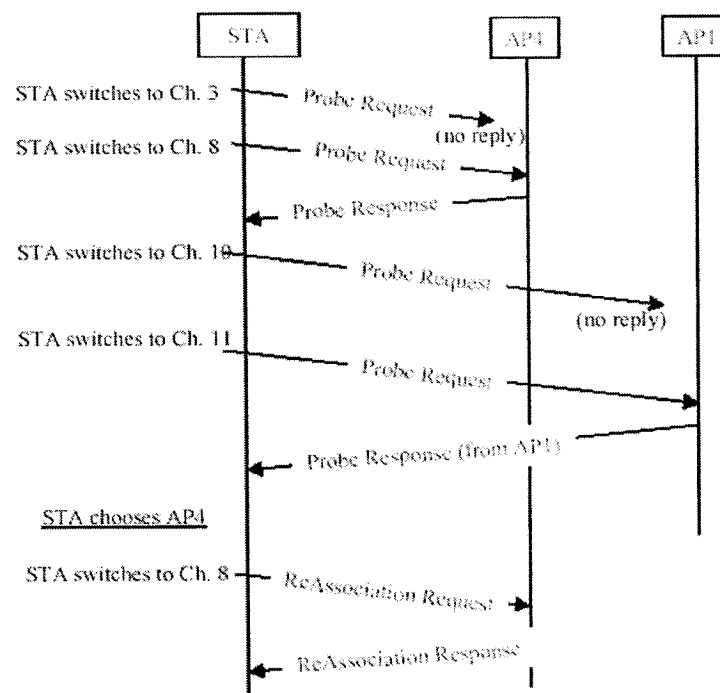


Figure 20. Handoff in 802.11 [44]

In WLAN minimum hierarchy in BSS and limited control message is used in order to save radio resource. STA does not know whether sub-network the new associated AP is in current or different sub-network. Because mobility is only supported within a single sub-network, it is not reliable to make a handoff between BSSs in different sub-networks interconnected by switch [44]. Additional protocol is needed to

enable the communication over the distributed system. This is why IEEE designed Inter-Access Point Protocol (IAPP).

The Inter-Access Point Protocol (IAPP) defines a service access point (SAP), service primitives and a set of protocols and functions to allow APs to interoperate on a common distribution system (DS). Figure 21 shows the AP architecture with IAPP. The IAPP is implemented on the top of IP layer so that it can work across router boundaries. IAPP packets can be transmitted between APs over TCP/UDP or Remote Authentication Dial-in User Service (RADIUS) protocol. The IAPP service can be access by AP Management entity (APME) through the IAPP SAP, which “allow APME to invoke IAPP service and receive indications of service invocations at other APs in a single ESS” [52]. There are four types of service primitives in SAP: requests, confirms, indications and response, which makes it possible for IAPP to perform some functions or communicate with RADIUS server and other APs in the DS [52].

The basic function of IAPP is to support handoff. The process of handoff in IAPP is composed of two procedures: announcement procedure and handoff procedure. Announcement procedure provides the identification of active APs in an ESS and coordinated management and configuration of APs. Handoff procedure notifies the old AP that a STA is re-associating with a new AP and updates layer 2 devices in the DS to properly forward frames to the re-associated STA. During handoff a STA assumes that it can forget the old association and only the current association is valid. The IAPP handoff procedure is interacted with the STAs ReAssociation process. After the ReAssociation request from the STA initiates a handoff, request from the new AP is sent to the old AP by using IAPP. Moreover, IAPP is used over wired network to tell change the association status. Any intervening bridges will be reconfigured to forward frames to the new AP for the reassociating STA [44].

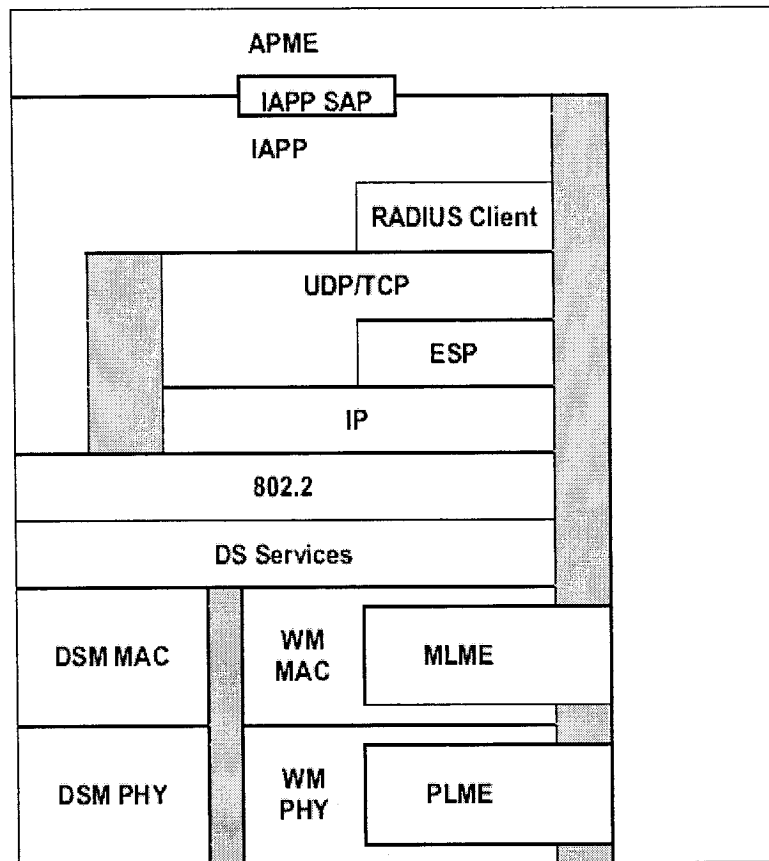


Figure 21. AP Architecture with IAPP [52]

To make a handoff IAPP will first notify the old AP that the STA will get controlled by a new AP, and then release the resources that the old AP possessed to keep the connection with STA, update its filter table to forward frames destined for the STA appropriately, discard or forward frames buffered for the STA in the old AP. At last, update filter tables of intermediate MAC-bridges to forward frames destined for the STA appropriately [44].

Two transfer protocols have been defined in IAPP, one for single logical LANs and another for multi LANs with router at boundaries. Mobile IP software is required for UE roaming across router boundaries. Management capability is configurable, depending on the parameters commonly used by an AP. The configurability makes it possible for all APs from different 802.11 vendors to operate consistently in a multi-vendor device environment. IAPP entities are responsible for interoperability issues during handoff in DS [44].

Fast handoffs can only be achieved when the mobile host keeps its IP address during moving across cells. Mobility management functionalities are implemented based on the following signaling messages: handoff initiation, handoff request propagation, handoff granted, new route setup, old route deletion, etc. The measurement option in WLAN physical layer is used for handoff management. This requires a centralized network element responsible for handoff decisions and WLAN does not provide RRM function as in hierarchical WCDMA [44].

3.6 Vertical Handoff Problem

It is known that a vertical handoff can only be a hard handoff. The trade-off between the number of unnecessary handoffs and the handoff delay still exists. Also, traditional “ping-pong” effects are more serious because the cost of vertical handoff is much higher than horizontal handoff.

Besides these traditional handoff problems, there are some new issues for the vertical handoff between 3G networks and WLAN

- Because 802.11 based WLAN technologies are totally different from WCDMA based 3G networks in terms of radio access methods, network protocol, etc, the handoff process will consume much more network resource, take longer period of time and result in higher call drop rate. On the other hand, WLAN provides higher bandwidth and less cost. We need to figure out how to evaluate the handoff.
- Vertical handoffs are involved with different network technologies, which have different bandwidth, charge policy, quality of service, power consumption and SNR, How to choose the network we are going to switch is a multi-criterion decision.
- The dwelling time within WLAN depends on the moving trajectory and velocity of the UE. If the dwelling time in each WLAN is very short, the UE has to make handoffs between WLAN and WCDMA frequently. This is another kind of serious ping-pong effect.
- The characteristics of the application and its requirements for bandwidth and network service are supposed to be considered when making a handoff decision.

- Subscribers are allowed to define their preferences and policies for vertical handoffs. 3G networks can automatically make a handoff decision according to the subscriber profile. But, in some situations, the subscriber's participation is necessary.
- To make a vertical handoff, the UE must be dual mode terminal. As we know, the battery power of UE is limited; this is why power control is so important in cellular network. If we keep both network interfaces active and measure the signal continually, UE will run out of battery in a short time. How to save power is a critical issue.
- The subscriber can initiate the handoff himself.

As mentioned in Chapter 1, current research on vertical handoffs are focused on the architecture and protocol design. Only a few publications on handoff decision making algorithm can be found. Also, all of the decision making algorithms are focused on the multi-criteria decision model. No complete solution for handoff decision making has been proposed.

Chapter 4

Proposal

Beyond 3G or 4G, wireless networks will be heterogeneous. This new era of wireless network has already made inroads because many telecommunication corporations are increasing investment on the R&D in this field and dual-mode (WCDMA and 802.11) user equipment (UE) has already shown up on the market. This thesis focuses on the decision making for vertical handoff between WCDMA based 3G cellular networks and 802.11 based WLAN. I have proposed a location aided vertical handoff architecture, handoff prediction and evaluation algorithms on SRNC (Serving RNC) side. Also, I have designed a multi-priority policy based decision making and signal detection algorithm on UE side.

4.1 Basic Idea of Location Aided Handoff

The first idea is to use location information. WLANs are typically confined within small geographic areas like campuses, airports, and buildings and most WLAN are security-enabled wireless networks, which can be accessed only by authorized users. To make seamless roaming between cellular networks and WLAN, how can UE know which WLAN it is allowed to access and where the best place to make the handoff is? Without aided information UE has to keep two network interfaces active and scan the radio signals continually, dramatically increasing the power consumption to make UE run out of battery power in a short time. Also without location information, the handoff is a blind handoff because UE has absolutely no idea of the coverage size or its dwelling time within the WLAN. Nor does the UE know whether the handoff can bring enough benefits to compensate the cost. In addition, the blindness will bring a serious “ping-pong” effect and the network overhead, caused by so many unnecessary vertical handoffs, cannot be ignored.

Fortunately 3GPP standards have defined many location based services that require 3G networks capable of tracking the UE location through A-GPS or U-TDOA technologies. It seems that 3G networks can navigate the vertical handoff intelligently by

using the UE location and WLAN information; however, the performance of current A-GPS technology is very poor in urban and indoor environments, where most WLAN is located. The location accuracy of current U-TDOA, as mentioned in Chapter 2, is only twenty meters. Under normal circumstances a ten meter accuracy is required to provide navigation service, so we cannot totally rely on the location information provided by 3G networks to make a handoff decision. As we know, the accuracy of location information provided by WLAN is one meter, which is accurate enough to navigate the handoff; therefore, my solution is to take advantage of both the location information provided by 3G networks and WLAN to make a good handoff decision.

There are two kinds of vertical handoffs: upward (from WLAN to 3G) and downward handoffs (from 3G to WLAN). Because the aim of a downward handoff is to take advantage of the high bandwidth and low cost of WLAN for better service, the subscriber may prefer to make a handoff only when the WLAN signal is strong enough to keep a good connection. Accuracy is more important than timeliness for downward handoff. Although 3G networks cannot provide the necessary accuracy location information (UE speed, moving direction, and position) to navigate a downward handoff, it can still use this information to estimate potential handoffs and notify UE to fetch exact location information provided by WLAN service for an accurate handoff decision. Also, its world-wide coverage characteristic makes 3G networks a qualified decision maker for vertical handoff. On the other hand, the reason for an upward handoff is the weak signal strength or poor signal quality of WLAN, which determines that upward handoff is time-sensitive. Lower call drop rate and better connections are more important than enjoying the high-speed and low-cost of WLAN, so we need to make the upward handoff at an accurate location and time. Fortunately prior to upward handoff, UE is connecting with WLAN, which can provide the exact position information to assist the handoff decision.

The second idea is to use pedestrian road maps. Pedestrian road maps include the layout of sidewalks and the structure of buildings covered by WLAN. The WLAN cell size is only 50-100 meters. If high-speed UE makes a handoff to WLAN, UE has to make horizontal handoffs frequently, which will ultimately increase the call drop rate and consume network resources. This means that the vertical handoff is only suitable for low

speed UE. Normally UE only moves along the sidewalks on the streets and enters or leaves the buildings through the exits. This constant moving pattern will help to estimate the trajectory of UE and make a more accurate handoff prediction. Also, we can get more accurate location information by mapping the location information provided by 3G networks on the pedestrian maps.

The third idea is to use WLAN coverage maps. It is very hard to get real-time WLAN coverage maps on SRNC side. As we know, radio signal strength is composed of deterministic components (path loss and shadow fading) and random component (Raleigh fading). The deterministic components that dominate the signal are relatively constant because building structures and obstacles are not changed over a short period of time. The random components only fluctuate within a small scope, so the non-real-time WLAN coverage map on SRNC can still be used for a handoff prediction. How to get the coverage map and pedestrian road map is beyond my thesis. Because WLAN signals and UE moving trajectories are relatively constant, the vertical handoffs are predictable and always happen in fixed locations. With the help of UE location information and WLAN coverage maps, we can avoid the “ping-pong” effect, solve the trade-off between handoff delay and the number of unnecessary handoffs in the traditional handoff algorithms.

In summary, the idea of my proposal in this thesis is to use WLAN coverage maps, the pedestrian road maps and location information provided by both 3G networks and WLAN to make decisions for vertical handoff.

4.2 System Architecture

We make the following assumptions before presenting the system architecture.

- a) UE has dual mode interfaces supporting both 3G and WLAN technologies.
- b) 3G Networks offer “always-on” service and cover all WLAN. When UE is connecting with WLAN, 3G networks can still communicate with UE.
- c) WLANs provide location service and UE has installed corresponding software. For example, we can install “Ekahau Positioning Engine” on AP side and “Ekahau Client” on UE side.
- d) 3G networks have WLAN coverage maps and pedestrian road maps

Figure 22 illustrates the system architecture for the location aided vertical handoff. This architecture is built mainly on the top of generic LCS (Location Service) architecture and the loosely coupled architecture for WLANs and 3G networks. SRNC (Serving RNC) includes the functionalities required to support 3GPP location service and is responsible for handoff prediction and evaluation. WLAN coverage maps and pedestrian road map are stored at the Map Information Server (MIS). SRNC can also get user preference from subscriber profiles. 3G operators can establish their own WLAN in hot spots, or cooperate with other WLAN providers in order to offer roaming service for their subscribers. Such accessible WLAN information, such as WLAN ID, technology parameters is stored in subscriber profiles to help SRNC decide if the approaching WLAN is available for this specific UE.

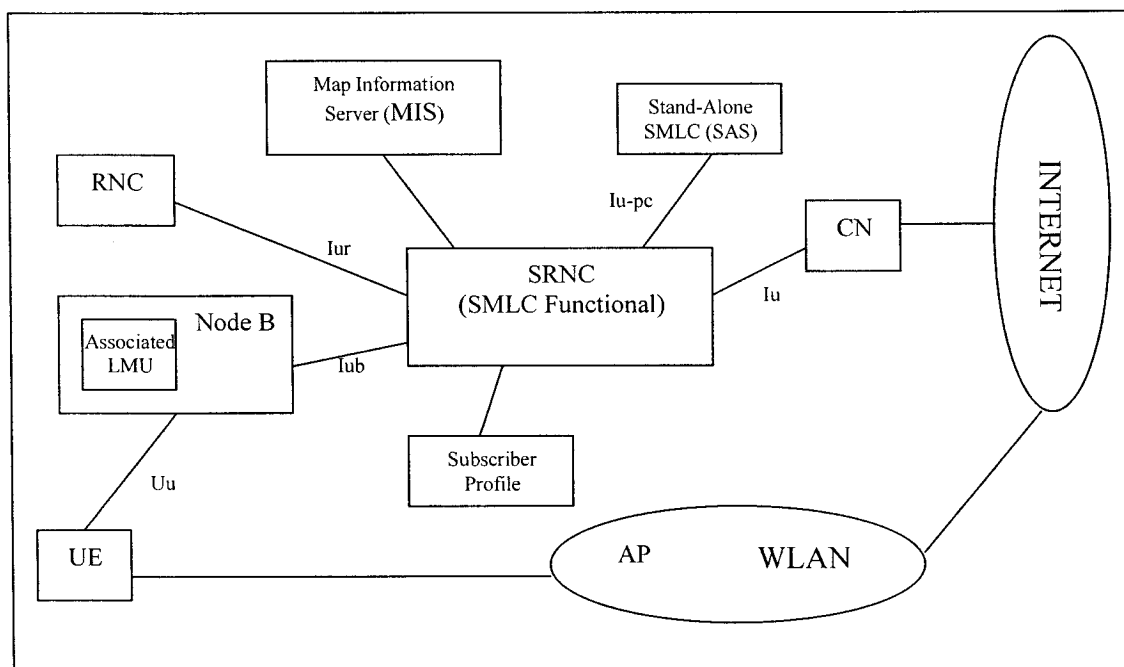


Figure 22. System Architecture for Vertical Handoff

The vertical handoff can be launched by the network seamlessly or by the UE itself in order to increase flexibility. Here a UE initiated handoff can be launched by either the subscriber or applications running on UE automatically; for example, the subscriber has defined a policy that all phone calls will go through 3G networks. During connections with WLAN, the UE will initialize an upward handoff to 3G networks when

the subscriber wants to make a phone call. We classify the vertical handoff into four categories: *network initialized downward (from 3G to WLAN)*, *network initialized upward (from WLAN to 3G)*, *UE initialized downward* and *UE initialized upward handoffs*. The network initiated handoffs are network navigated and UE controlled handoff. UE does not know the information of accessible WLANs, such as location, coverage size, charging policy, or technical parameters (bandwidth, modulation, frequency, etc.), while SRNC can get such information easily. Also, because the UE battery capacity is limited, it is not efficient to keep WLAN interface active continually. The ideal method is to let UE turn on its WLAN interface when WLAN is available. These factors will determine that the handoff is network navigated. Horizontal handoffs are network controlled because uplink signals can be measured to determine the handoff time. For vertical handoffs only UE can detect signals of both 3G networks and WLAN simultaneously. Also, the handoff decision is relevant to the UE application characteristics and subscriber's preference. In addition, vertical handoff may be launched by UE instead of the networks. Therefore, the network initiated handoffs are also UE controlled handoffs. UE initiated handoffs also need the SRNC to make evaluations.

A *UE initialized upward handoff* is straightforward, which does not need any decision algorithm and simply executes the handoff procedures because the 3G networks provide "always-on" service and can be accessed anywhere. A *UE initialized downward handoff* will be launched if the subscriber wants to access WLAN, or run some applications that need to make a handoff. UE does not need to send a handoff evaluation request to SRNC at the beginning in order to decrease the network traffic. UE simply turns on its WLAN interface and measures the signal for an interval T . If the signal is not strong enough UE will turn off the interface. Otherwise, UE will get its accurate location information from AP and send it to SRNC for handoff prediction and evaluation, then UE will start the signal detection algorithm (see the algorithm in section 4.4) immediately to decrease handoff delay. SRNC will make handoff evaluation according to UE location information, moving speed, moving direction, and WLAN coverage maps. I will give a detailed explanation in section 4.3. UE will make a handoff to WLAN after receiving the handoff command from SRNC. Figure 23 is the sequence diagram of the UE initialized downward handoff.

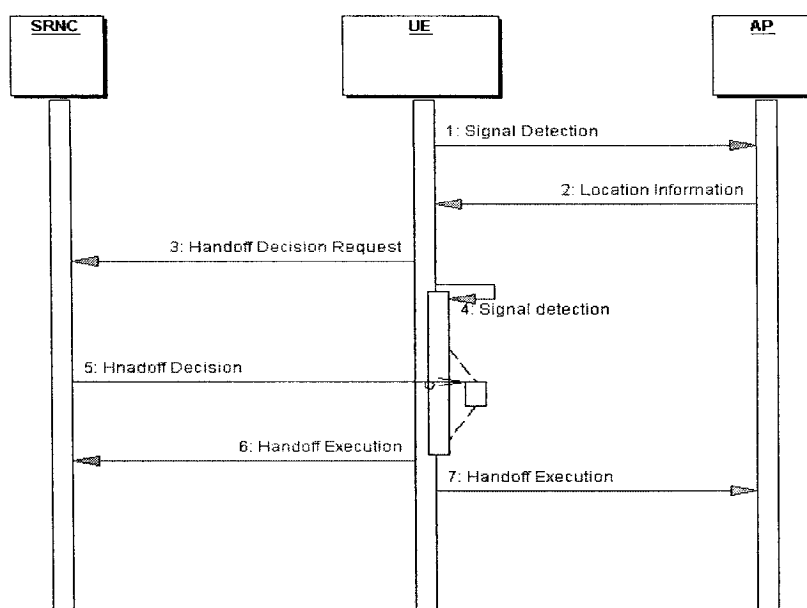


Figure 23. UE Initiated Downward Handoff

Network initiated downward handoff is much more complex than UE initiated handoff. Figure 24 shows a simplified model: UE is moving toward a WLAN along a straight sidewalk AF. The subscriber can choose to permit or block the seamless vertical handoff service and this information will be stored in the subscriber profile. SRNC will not predict and evaluate the possible downward handoff automatically if this service is blocked. In current 3GPP standards CN will send location requests periodically to SRNC, which will calculate the UE location after retrieving measurement results from LMU. Then SRNC will make a handoff prediction (the algorithm in section 4.3) by using this location information, WLAN coverage maps and UE moving pattern (the probability of different path). If a potential handoff has been found, SRNC will evaluate it by using the algorithm elaborated in section 4.3. Network initiated downward handoff is a network navigated handoff. In figure 24, if the predicted handoff is valuable, SRNC will notify UE at point A: you are approaching a WLAN with velocity V , wake up your WLAN interface and start to scan beacons. UE will make a handoff decision by using the algorithm in section 4.5. UE will turn on the WLAN interface and start signal scanning if the handoff is desirable. At point B SRNC will tell UE that you are close to a WLAN boundary, increase the signal scanning rate. Also, SRNC will ask CN to request location

information of the UE more frequently. At point C, UE gets accurate location information from AP because UE is pretty close to the WLAN boundary and sends it back to SRNC. SRNC will predict and evaluate the handoff by using the accurate location information and send handoff execution, or handoff cancellation command to UE. After receiving a handoff execution command, UE will start the signal detection algorithm in section 4.4. If the algorithm is successfully finished at point D, the UE will make a handoff to WLAN. During the transition period the SRNC will evaluate the handoff again if the UE changes its moving direction or velocity greatly.

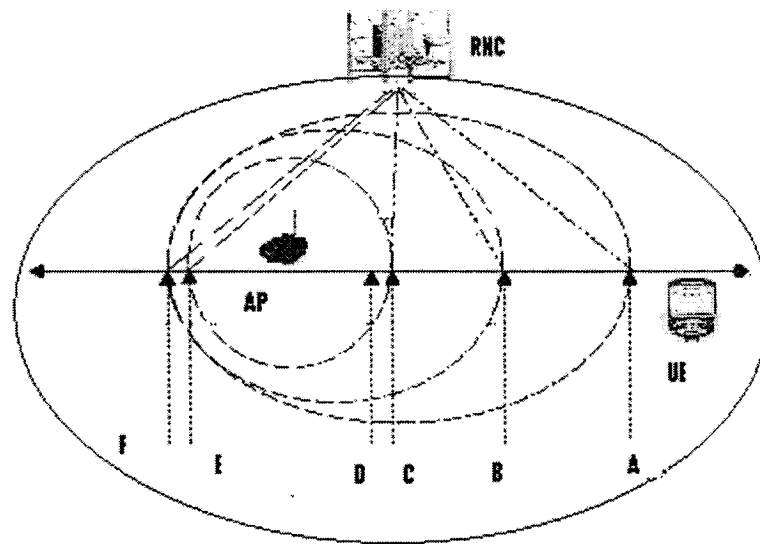


Figure 24. Network Initialized Handoff

Figure 25 is the sequence diagram for a successful network initialized downward handoff. This situation will happen if SRNC predicts a valuable handoff; UE makes a handoff decision to WLAN and the signal detection algorithm finds WLAN with strong and stable radio signals. UE will not turn on the WLAN interface and just send a “no-handoff” message to SRNC if the handoff is not necessary at this moment. SRNC will not send any handoff message to the UE for a period of time. Figure 26 shows this scenario.

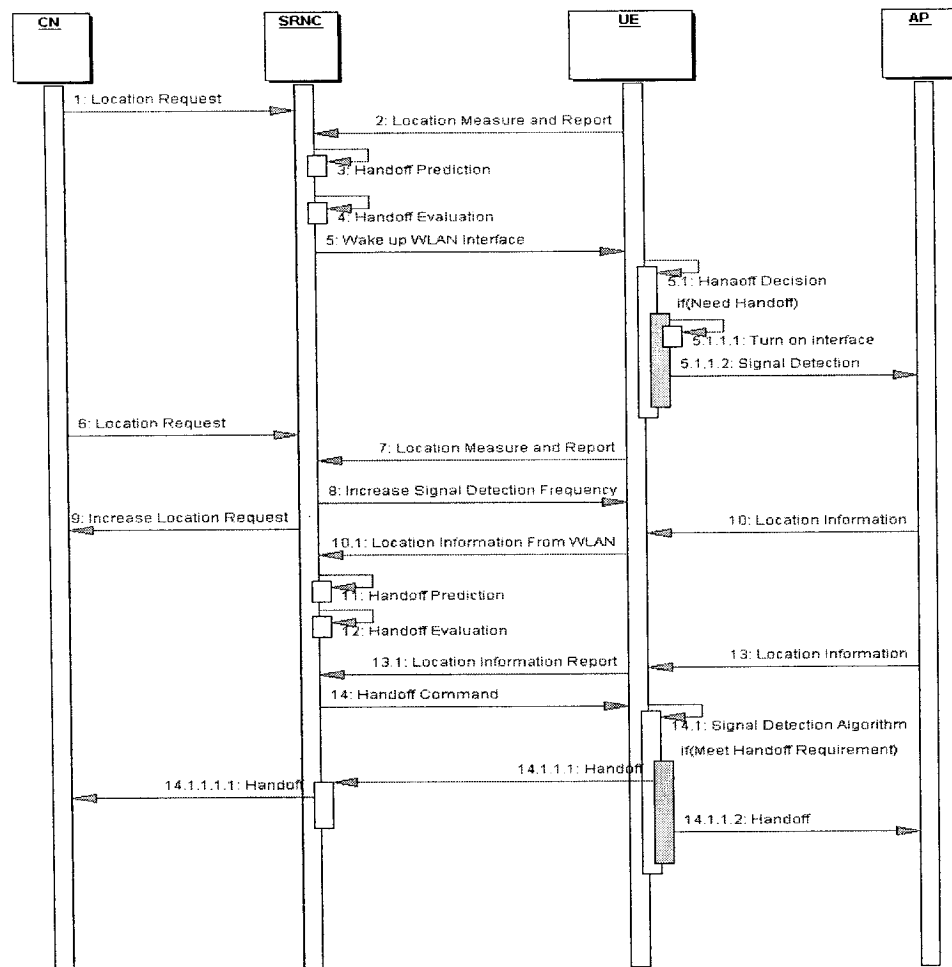


Figure 25. Successful Network Initialized Downward Handoff

SRNC will notify UE to turn off the WLAN interface if UE changes the moving direction and moves away from the WLAN after turning on its WLAN interface. Also, SRNC is supposed to tell UE to adjust the scanning frequency and ask CN to change the location requesting frequency if the moving speed of UE is changed. As we know, SRNC will evaluate the handoff again after receiving the accurate location information provided by WLAN.

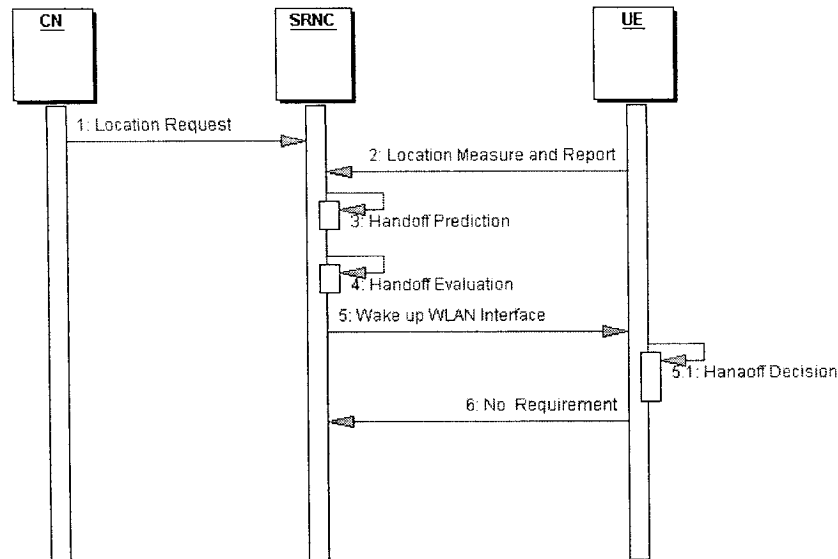


Figure 26. No Downward Handoff on UE side

Given that UE has received the handoff execution command from SRNC, however, if the signal detection algorithm shows a weak signal strength or poor signal quality (SNR), UE will send feedback to SRNC. SRNC will recheck the location and WLAN coverage maps ensure it is a correct handoff decision. SRNC will wait for the next message from UE if SRNC determines it is a correct handoff. The second signal detection failure message will force SRNC to make a record of the status of WLAN. UE will turn off its WLAN interface. This scenario is shown in Figure 27.

Network initialized upward handoff is time-sensitive because it is triggered by the weak, or low quality signals that may result in disconnection. When UE moves close to the boundary of WLAN, as indicated by point E in Figure 24, SRNC will be aware of it because UE can get its accurate location information from WLAN and report it to SRNC periodically. UE will start the signal detection algorithm in section 4.4 after a handoff suggestion is received from SRNC. When the signals are strong enough for a good connection, UE will launch an upward handoff and notify SRNC and AP to execute the handoff process. Figure 28 provides the sequence diagram for this scenario. SRNC is supposed to evaluate the handoff decision again if it does not receive UE's response within a period of T. However, UE should not be totally dependent on the handoff

suggestion from RNC. When the signal gets weak, UE should make a decision and launch the upward handoff itself.

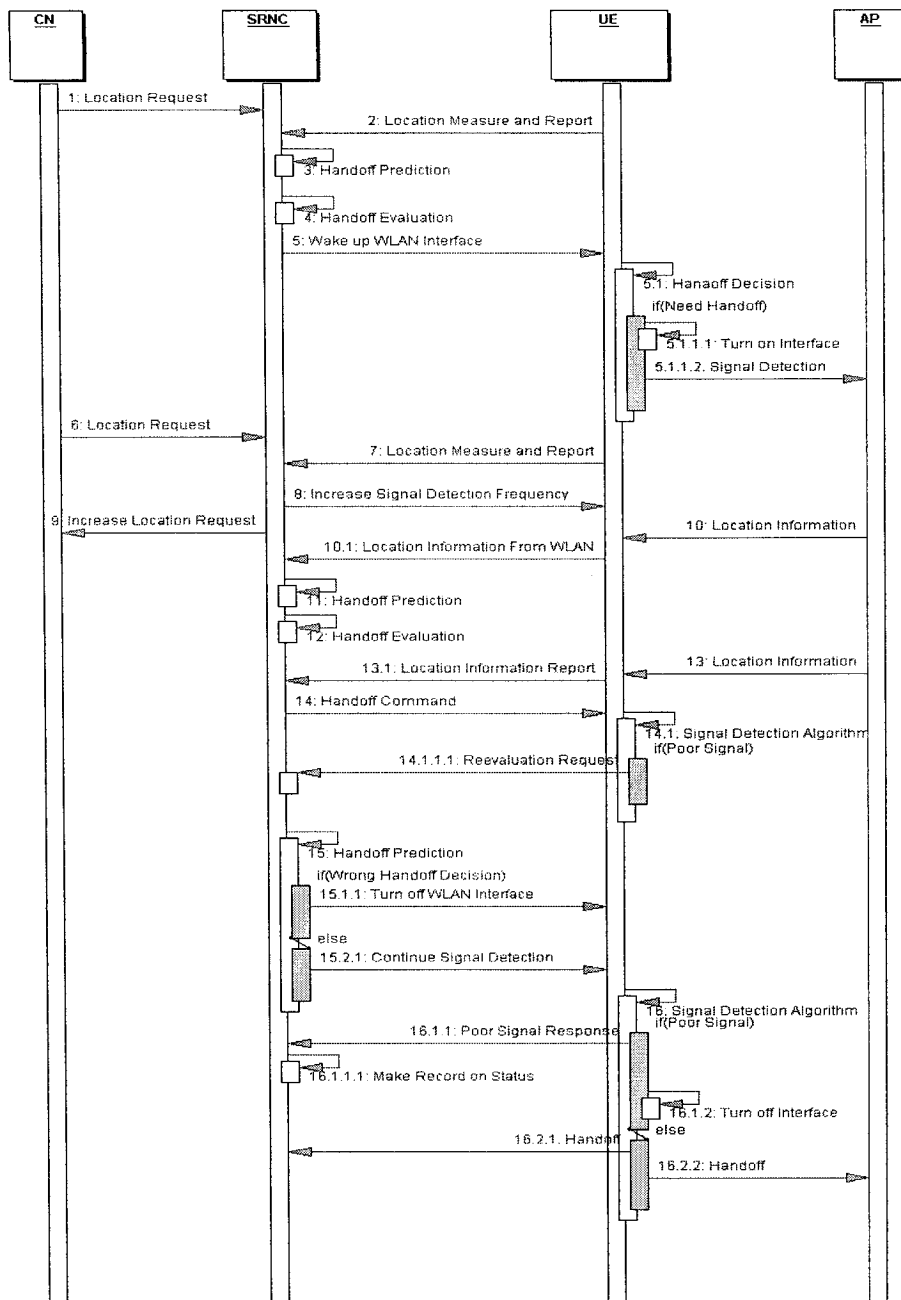


Figure 27. WLAN Signal Detection Failure

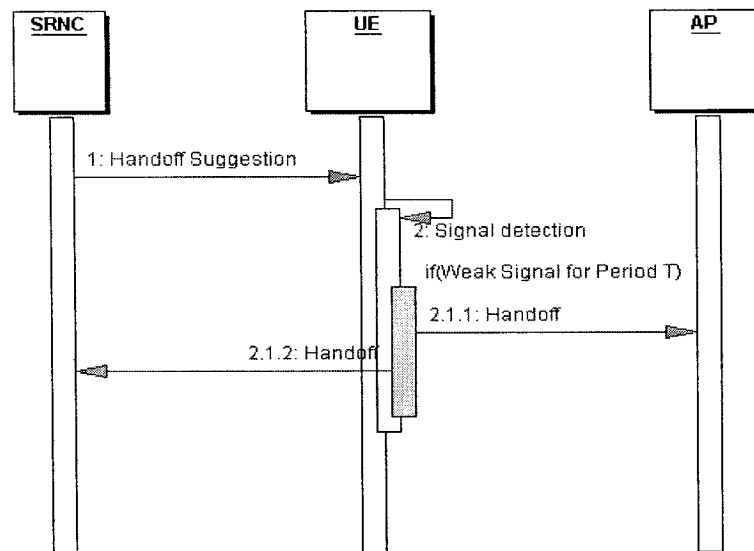


Figure 28. Network Initialized Upward Handoff

4.3 SRNC Handoff Decision

Given the real-time location information of UE, WLAN coverage maps, and pedestrian road maps, SRNC is supposed to navigate UE to make a valuable handoff from 3G networks to WLAN. The decision process on SRNC side includes two stages. The first stage is to predict the potential handoff, and the second is to evaluate its profitability.

4.3.1 Handoff Prediction

How can we predict a handoff? The straightforward way is to extend the current moving trajectory of UE in a straight line. If there is an intersection with WLAN boundary, the UE will be within WLAN coverage scope and a handoff might be launched. The estimation time to enter WLAN can be calculated by the UE's current speed and the distance from the WLAN boundary in the extended line. Even if we only consider an outdoor environment this prediction algorithm is too simple and ideal, because UE is normally moving along a path, which is consisted of several road segments instead of one straight line. To make a better handoff prediction and estimation of the correct time to notify UE for a handoff preparation, pedestrian road topology, statistical moving pattern, UE location coordinate, moving direction, and speed are all supposed to be considered.

In order to simplify the model we assume the UE only moves along paths on the pedestrian road maps. Figure 29 shows a simple example, where green cycles represent WLAN; point A, B, C, D, E, F, and G represent intersections of road segments; and line AB, BC, etc. represent road segments. The segments are very short because WLANs are always located in urban and campus areas. Also, the accuracy of current 3G location technology in these areas is around 20 meters, so we are supposed to prepare a handoff when UE is still a little bit further from the WLAN boundary. We can define distance D as the measuring radius from WLAN boundary. In Figure 29 the red arc represents the WLAN1 measuring scope, within which all of segments should be considered. SRNC is responsible to calculate the probability to enter WLAN1 and the time period that it will take to reach WLAN1 for all UEs moving in its serving area.

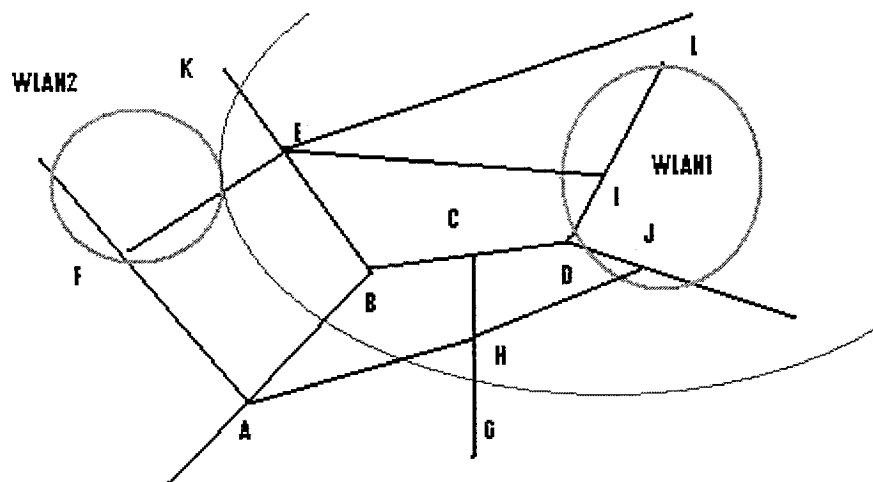


Figure 29. Using Pedestrian Road Map for Handoff Prediction

Assuming a UE is moving from A to B, it may walk along path1 (BE->EI), path2 (BC->CD->DI), path3 (BC->CD->DJ) or path4 (BC->CH->HJ) to enter WLAN1. Also, it may go along path5 (BE->EK), path6 (BE->EL) or path7 (BC->CH->CG) to be away from WLAN1. The probability for each path is different. In addition, the dwelling times in WLAN1 are different if UE takes different road segments, such as DL or DJ, to pass the WLAN coverage scope.

The first step for handoff prediction is to get the probability of different paths. For each segment S we need to calculate the probabilities for all paths beginning with S. Take

segment AB as an example, we will get the moving probabilities for all paths beginning with AB and passing through WLAN1 and WLAN2. Also we need to probability of any paths away from any WLANs. The probability of path 'AB->BC->CD->DJ' is represented by $P(s_4=DJ \mid s_3=CD, s_2=BC, s_1=AB)$ and the probability of path 'AB->BE->EI->IL' is represented by $P(s_4=IL \mid s_3=EI, s_2=BE, s_1=AB)$. Because the road topology, WLAN coverage, and UE moving pattern are stable for a long time, we do not need to calculate these data often. In SRNC we can store the moving trajectory of UE in this area for a period of time. It is not hard to get such information by using these statistics. Next I will explain how to use this data to predict the vertical handoff. The algorithm is as follows:

1. SRNC calculates the UE location, velocity, and direction according to the measurement results. Comparing with the pedestrian road maps, SRNC estimates the location of UE again and maps it onto a road segment.
2. WLAN coverage maps are checked. If UE is within WLAN coverage, the subscriber profile is checked to know whether this WLAN is entitled to be connected or not. SRNC then makes evaluation of this handoff according to the method in section 4.3.2. If it is a valuable handoff, the handoff command is sent to UE, otherwise, UE cancels the handoff.
3. The algorithm will be stopped if UE is outside of any WLAN measuring scope.
4. If UE is within the measuring scope of a set of WLAN set S, then:
 - 4.1 The subscriber file is checked and only the authorized WLANs among WLAN set S are selected. The probability P_i to move towards each of these WLANs is calculated.
 - 4.2 The WLAN with the largest probability P is selected.
 - 4.3 A probability threshold that is the minimum probability value to be considered as a candidate WLAN is predefined. The algorithm is exited if P is less than this probability threshold, otherwise continue the following steps
 - 4.4 The remaining path length to the WLAN boundary is estimated:

$$L_{est} = \sum_{i=1}^n P_i * (c + \sum_{j=1}^{k-1} l_j), \text{ where } n \text{ is the total number of paths towards the chosen}$$

WLAN, P_i is the probability of path i , c is the remaining length of the current segment, l is the length of the segment j in the path I and k is the number of segment in the path i (including the current segment)

4.5 SRNC calculates the time that will take UE to enter this WLAN by using the formula $T_{est} = L_{est} / v$, where L_{est} is the remaining path length to the WLAN boundary and v is the velocity of the UE.

4.6 SRNC will notify UE to turn on the WLAN interface if $T_{est} < T_{thresh}$, where T_{thresh} is the predefined minimum time to begin scanning the WLAN signal.

4.7 SRNC will notify CN to increase location measurement rate if $T_{est} < T_{cn}$, where T_{cn} is the predefined time when the frequency of the location measurement is supposed to be increased.

4.8 SRNC will notify UE to make handoff if $T_{est} < T_{handoff}$, where $T_{handoff}$ is the predefined time to start the handoff preparation.

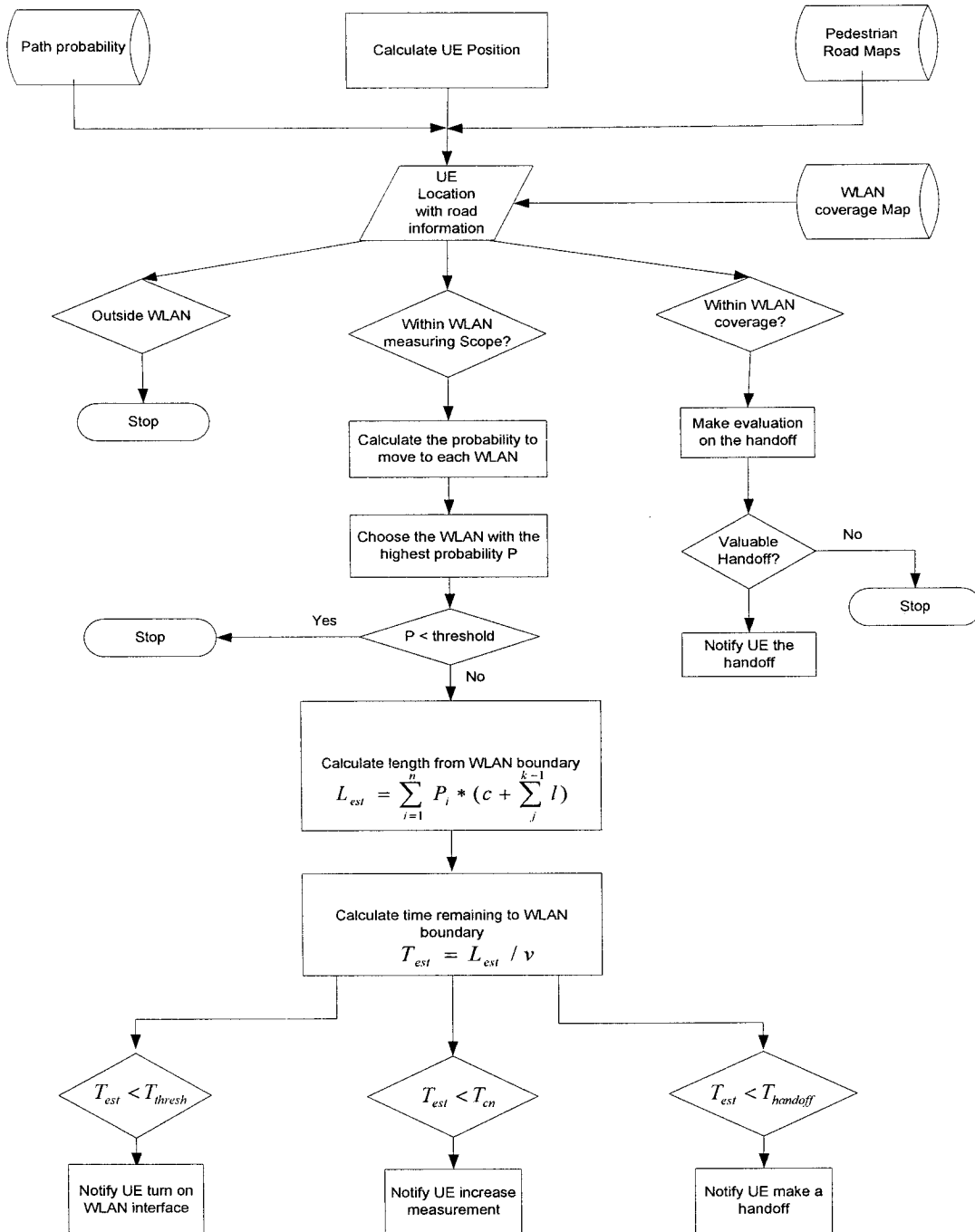


Figure 30. Flow Chart of Handoff Prediction algorithm

4.3.2 Handoff Evaluation

We are going to use dwelling time, which is relevant to UE speed and length of segments within WLAN, to evaluate whether the handoff is valuable.

The goal of handoff from 3G Networks to WLAN is to take advantage of the higher bandwidth and lower price of WLAN; however, the vertical handoff itself will take some time, consume network resources, and may result in high call drop rates, so there is a trade-off between the cost and benefits of the handoff. Now SRNC is aware that UE is moving towards a possible handoff area, but is this handoff valuable? As mentioned in Chapter 3, a vertical handoff decision is a multi-criteria decision; bandwidth, price, power consumption, network load, application character, user's preference, etc. should all be considered. With respect to SRNC side, we are only concerned with bandwidth and price. Other factors will be considered on the UE side. We can define the network overall cost as $f = N(B, C)$, where f is the overall cost for either 3G networks or WLAN, B is the bandwidth, and C is the charge rate. We can define the cost formula as:

$$f_n = w_b \ln(1/B_n) + w_c \ln(C_n + 1) \quad (w_b + w_c = 1)$$

where w_b is the coefficient of bandwidth, and w_c is the coefficient of charge rate. The subscriber can define these coefficients in his/her profile located in SRNC. If he/she only concerns the throughput, he/she will set $w_b=1$ and $w_c=0$; while if he/she simply wants to connect to the cheapest network, he/she can set $w_b=0$ and $w_c=1$. If network A has twice as much bandwidth as network B, but twice as expensive as the network B, the subscriber will think it equal good. This means that the overall cost functions should be the same. Because $\text{Log}(a) - \text{Log}(b) = \text{Log}(a/b)$, logarithm function can reflect this logic. Therefore, we choose log as the normalization function for each factors [18]. We can add other factors in the overall formula.

Normally WLANs have a much higher data rate but much lower cost than 3G networks, but a vertical handoff will cause a time delay T_{HANDOFF} . The benefit cannot compensate for the handoff cost if UE only connects with WLAN for a very short time. We need to calculate the minimum dwelling time (MDT) to connect with WLAN. We

ignore the horizontal handoff time in WLAN in order to simplify the calculation. If we only consider the bandwidth, we have a formula $(B_{WLAN} - B_{3G}) * T_{WLAN} \geq B_{3G} * T_{HANDOFF}$, in which B_{WLAN} is the WLAN bandwidth, B_{3G} is the bandwidth of 3G networks, and T_{WLAN} is the dwelling time in WLAN. Let $\lambda = B_{WLAN} / B_{3G}$, we get $T_{WLAN} \geq T_{HANDOFF} / (\lambda - 1)$. Then $MDT = T_{WLAN} + T_{HANDOFF} = T_{HANDOFF} (1 + 1/(\lambda - 1))$. We can generalize the calculation of T_{WLAN} for the overall cost function above as $T_{WLAN} = T_{HANDOFF} / (\exp(f_{3G} - f_{WLAN}) - 1)$ [18]. So we can get the following MDT formula:

$$MDT = T_{HANDOFF} * \left(1 + \frac{1}{\exp(f_{3G} - f_{WLAN}) - 1}\right).$$

We need to multiply a coefficient γ ($\gamma > 1$), which is an empirical parameter, because the vertical handoff brings extra network overheads and a higher call drop rate. The MDT then becomes:

$$MDT = \gamma * T_{HANDOFF} * \left(1 + \frac{1}{\exp(f_{3G} - f_{WLAN}) - 1}\right).$$

SRNC can get the probability P_i for path i according to statistics information. Then SRNC will calculate the estimated path length when UE is moving through the WLAN coverage area as $L_{ave} = \sum P_i * L_i$, in which L_i is the length of path i within WLAN and P_i is the probability to take path i . Divided by UE velocity we can get the estimating dwelling time $T_d = L_{ave} / V$ in WLAN (V is the velocity of UE). If T_d is greater than MDT then SRNC will notify UE that there is a valuable handoff, otherwise it is not a valuable handoff.

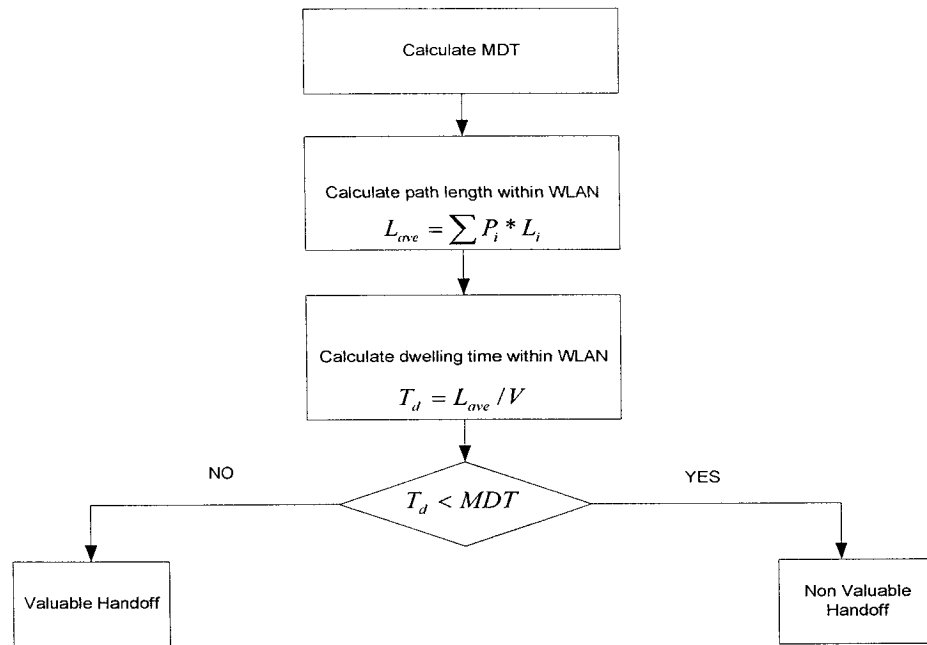


Figure 31. Flow Chart of Handoff evaluation algorithm

4.4 UE Signal Detection

Signal detection is not such an important issue as horizontal handoff because SRNC has location information and WLAN coverage maps, which can navigate correct handoffs. In horizontal signal detection algorithm, the RSS from different Node Bs should be compared as mentioned in Charter 3 by using hysteresis, time period and threshold etc. There is a trade-off between the handoff number and hysteresis or time period. We do not need to compare the relative RSS in vertical handoff because they are totally different wireless technologies and there is no any meaning to compare the RSS between 3G networks and WLANs. Threshold K is defined as the minimum received signal strength (RSS) that can guarantee a good connection with WLAN. We also defined the RSS hysteresis H. SRNC will calculate a time period T, which is dependent on the speed and moving direction of UE, and pass it to the UE side. In Figure 32, D as the distance of transition area, where RSS fluctuates around R. Only if RSS is larger than $K + H$ for period T, the vertical handoff can be launched. In addition to RSS data transmission rates and the signal quality in terms of signal-to-noise ratio (SNR) should also be considered

because different applications have different requirements on SNR and data transmission rates. We need to check which kind of applications trigger the handoff.

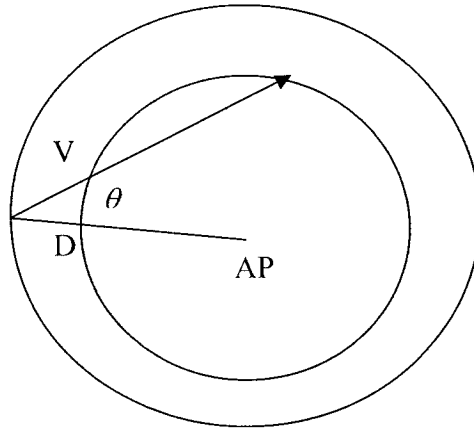


Figure 32. Signal Detection

The signal detection algorithm is shown as follows:

1. SRNC calculates the transition dwelling time $T = D / (V * \cos \theta)$ on transition area, where V is the UE speed, D is the width of transition area, and θ is the angle between moving direction and AP direction as shown in Figure 32. UE gets the SNR and data transmission rate requirement of the application that triggers this handoff.
2. The signal RSS is measured until RSS is above threshold K plus hysteresis H
3. If the RSS is above K plus H for period of T then step 5 is executed, otherwise the algorithm goes back to step 2.
4. If the RSS is less than K plus H , it goes back to step 2 and sets measuring time period as 0.
5. If the SNR and data rate meet the application requirements, then the handoff process is launched. Otherwise, report is sent to the subscriber about the network condition.

In case of upward handoff, a handoff process will be launched if the RSS is larger than threshold K but less than threshold K plus hysteresis H for period of T after UE receives “handoff suggestion” from RNC.

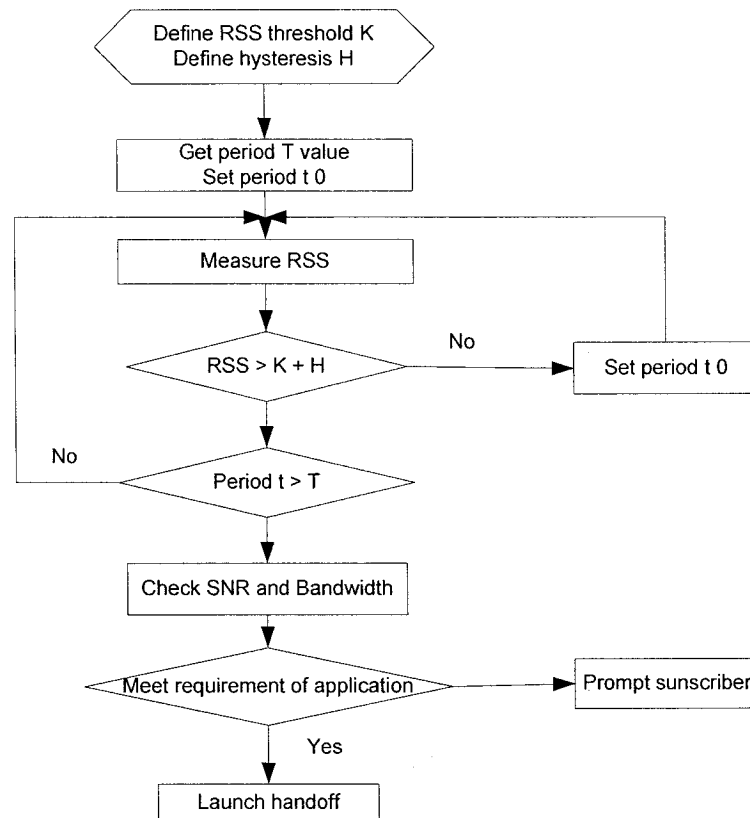


Figure 33. Flow Chart of Signal Detection Algorithm

4.5 UE Handoff Decision

With reference to the UE side the battery status, application characteristics, and user's preference should all be considered. There are two kinds of policies: system and user defined policies. The system will define some default policies include "no handoff during phone call", "block roaming to WLAN", "set phone call with high priority", etc.. These policies have a higher priority than user defined policies. The subscribers can change the settings of these system policies and can also define their own policies, which have lower priority. Every time UE receives the handoff suggestion from SRNC, the handoff decision algorithm will check which kinds of applications are running on the UE, the setting of system policies and the user defined policies. If a handoff is preferred UE will turn on the WLAN interface to detect WLAN signals and send SRNC a response to accept the handoff suggestion. Otherwise a "no-handoff" message is sent back to SRNC. If the subscriber or the applications running on the UE want to launch a handoff, these

policies are also needed to be checked first. If there is a conflict, a warning message is supposed to be displayed to prompt the subscriber involved with the handoff decision.

3GPP standards divide wireless applications into four classes: background (FTP, etc.), streaming (Video, Audio, etc.), interactive (Telnet, Yahoo messenger, MSN, etc.), and conversational applications. We have defined five accessing preference options for each kind of application: “Only WLAN”, “Only 3G”, “WLAN Preferred”, “3G Preferred” and “No Preference”. “Only WLAN” indicates this application can only be running through WLAN interface, a handoff to 3G networks will terminate this application. This application cannot be launched if WLAN is not available. “WLAN Preferred” indicates UE is supposed to make a handoff to WLAN if it is available. This kind of application will trigger a handoff to WLAN when available; otherwise, it will go through 3G networks. “No Preference” indicates the application can be running through current networks and no handoff is needed. “Only 3G” and “3G Preferred” have the similar meanings as “Only WLAN” and “WLAN Preferred” respectively. Network initialized downward handoffs are permitted if there is at least one “WLAN Preferred” application running in UE, or conversational application is defined as “WLAN preferred”, otherwise, no handoff will be made to avoid wasting network resource. We can set “WLAN Preferred” as the default option for the first three kinds of applications. It may be better to set a default choice for conversational application as “3G preferred” because the subscriber may prefer to make a phone call through 3G networks. The system is supposed to prompt user to set different priority on these policies if there are preference conflicts.

4.6 Simulation

It is hard to simulate the vertical handoff because we do not have the network and hardware environments. The current network simulators, like NS2, OMNeT++, QualNet, OPNET, etc. do not fully support the handoff between WLAN and 3G networks. I used a simplified model to evaluate my proposal in this thesis. I compared location aided and non-location aided vertical handoff by using Matlab in the following aspects: the number of handoffs, battery consumption, drop call rate, handoff delay, and the advantage of road topology.

There are no location information and WLAN coverage maps for non-location aided vertical handoffs, therefore UE has to keep WLAN interface active continually. When the UE is moving toward a WLAN, a downward vertical handoff will be launched if the RSS is greater than the threshold plus hysteresis H1 for a time period of T. The threshold is the minimum RSS that can keep good connection with WLAN and has the same value with the location aided handoff algorithm. The value of hysteresis in non-location aided handoff algorithm is also equal to that of the location aided algorithm. When the UE is moving out of WLAN, an upward vertical handoff is supposed to be executed if the RSS is less than threshold plus hysteresis H2 for T second. Hysteresis H1 is either more than H2 or equal to H2.

In [50] and [53], Tripathi and Ylianttila use an empirical path loss model, called “two slope model”, for their handoff simulations. In this model, RSS at distance d from an access point is given by: $RSS(d) = P_t - (10a \log d + 10b \log d / g) + S(d)$, in which P_t is the transmission power of the access point, and d is the distance from the AP. The parameters a , b and g are defined for path loss ($a=2$, $b=2$ and $g=150m$). $S(d)$ is a correlated log-normal shadow fading. To simplify the model let $S(d) = X_\delta$, which is a Gaussian random variable with zero mean and δ^2 variance ($\delta^2=1$). Figure 34 is the simplified WLAN RSS distribution for a place from 150 meters to 80 meters away from the AP. P_t is defined as 50 watt and sampling rate as 100 samples/meter. The Y coordinate is Received Signal Strength (RSS) with unit db. The X coordinate is the

distance from AP. The distance is 150 meters if x is equal to 0, while it is 80 meters if x is equal to 7000.

This model will be deployed to make evaluations on both location aided vertical handoff proposal and non location aided solution. We assume the RSS threshold for the handoff is 12db. WLAN coverage radius is 100 meters and the transition area is between 100-150 meters as Figure 35 shown. AP is located at Point O. UE is only moving along path AB->BH or path AB->BG. Segment BH only pass through the transition area and no desirable handoff should be launched.

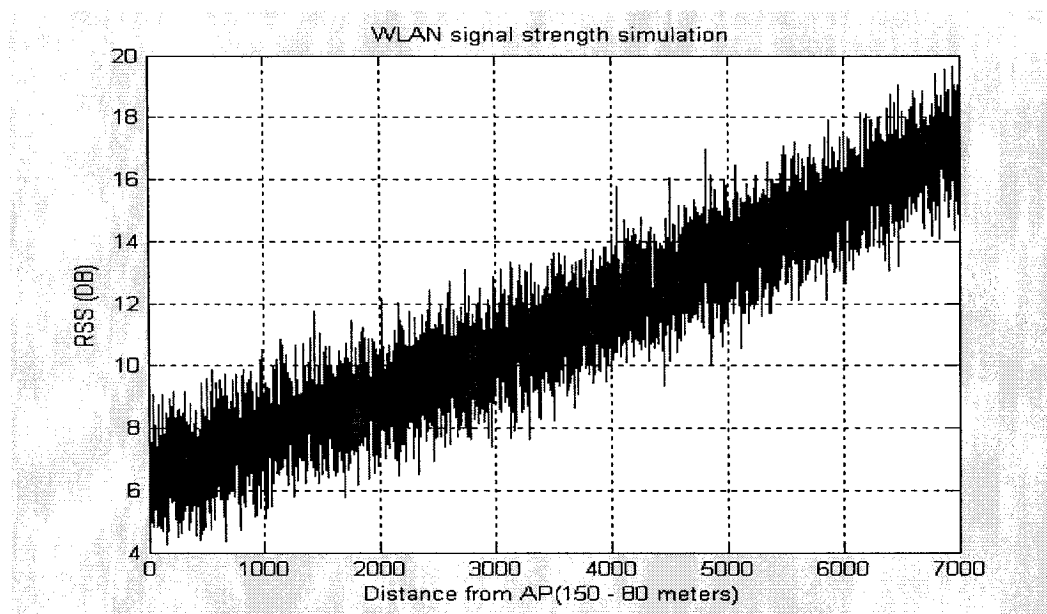


Figure 34. WLAN Signal Simplified Simulation

4.6.1. The Number of Handoffs

Scenario 1: Assume UE is moving towards WLAN along AO in Figure 35 at a speed of 1 meter/second. A downward handoff is supposed to be launched if the signal strength is above the threshold by H for T seconds. We simulated the moving-in scenario (handoff from 3G to WLAN) for both non-location aided handoff algorithm and location aided algorithm 100 times each. For each algorithm we made simulations using two hysteresis values (0.5 and 1). In Figure 36, X coordinate is the time period T and Y coordinate is the number of handoffs. The upper sub-figure is for non-location aided handoff and the lower is for location aided handoff. This figure shows the trade-off between the handoff number

and hysteresis, or time period T , which is a typical problem in traditional (non-location aided) handoff algorithm. The trade-off phenomena in non location aided handoff algorithm are much more obvious than in the location aided algorithm, which has a better solution to this trade-off. Also, the number of handoffs decreases greatly with the aid of location information, especially when the hysteresis and time period of T are small. Therefore, “Ping-Pong” effect gets effectively controlled.

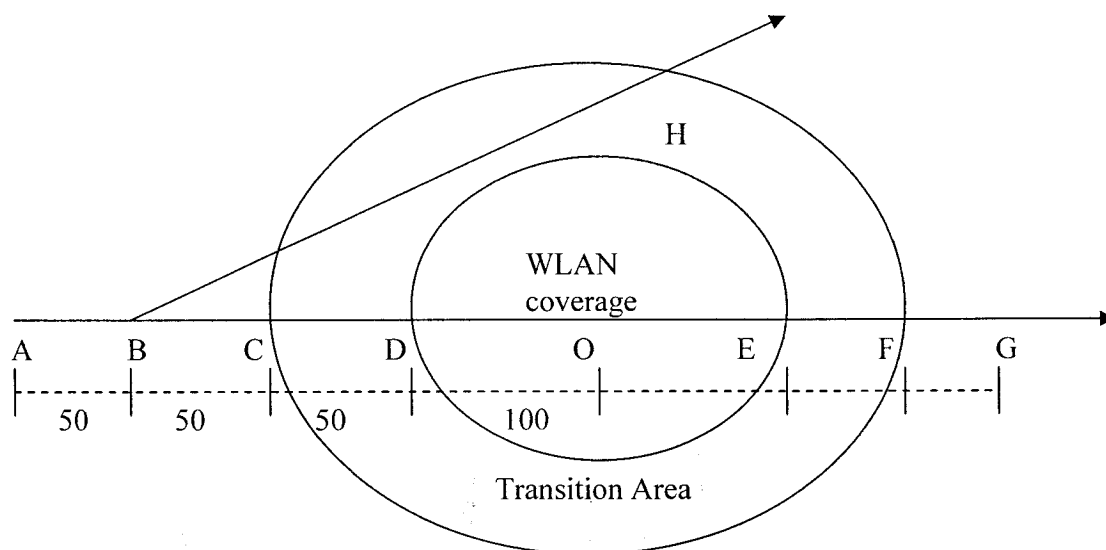


Figure 35. UE Moving Path

Scenario 2: In Figure 35 UE is moving along BH to pass the WLAN transition area. The UE can get accurate location information from AP when it is close to the WLAN. After UE reports the AP ID and the relative location information from AP to SRNC, SRNC can calculate the accurate location information to navigate the handoff. There is no valuable handoff in this scenario because BH is totally within WLAN transition area. The location aided handoff algorithm does not launch any handoff, which is what we really expected. On the other hand, there are serious “Ping-Pong” effects in non-location aided handoff algorithm especially when T is small.

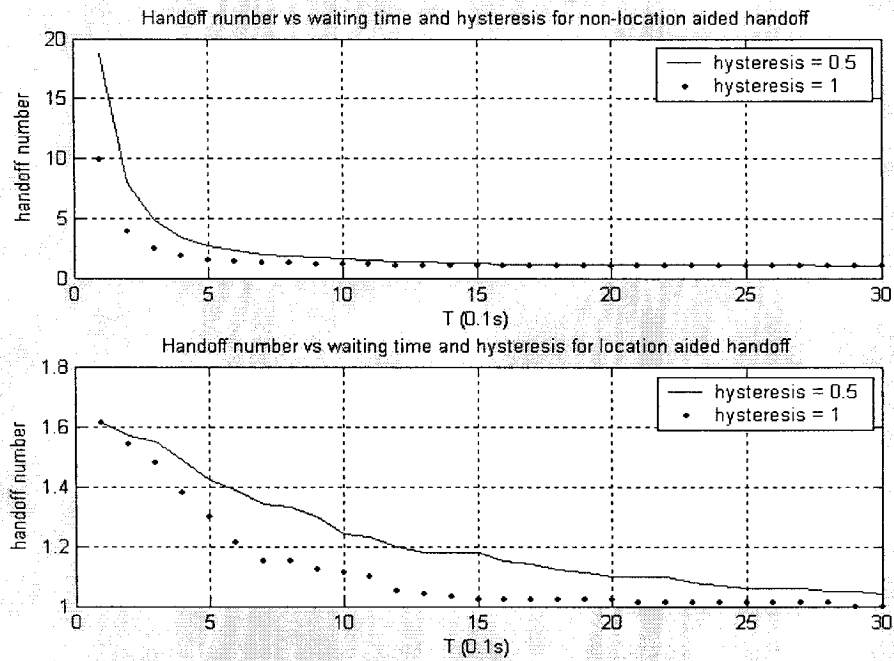


Figure 36. Number of Handoff

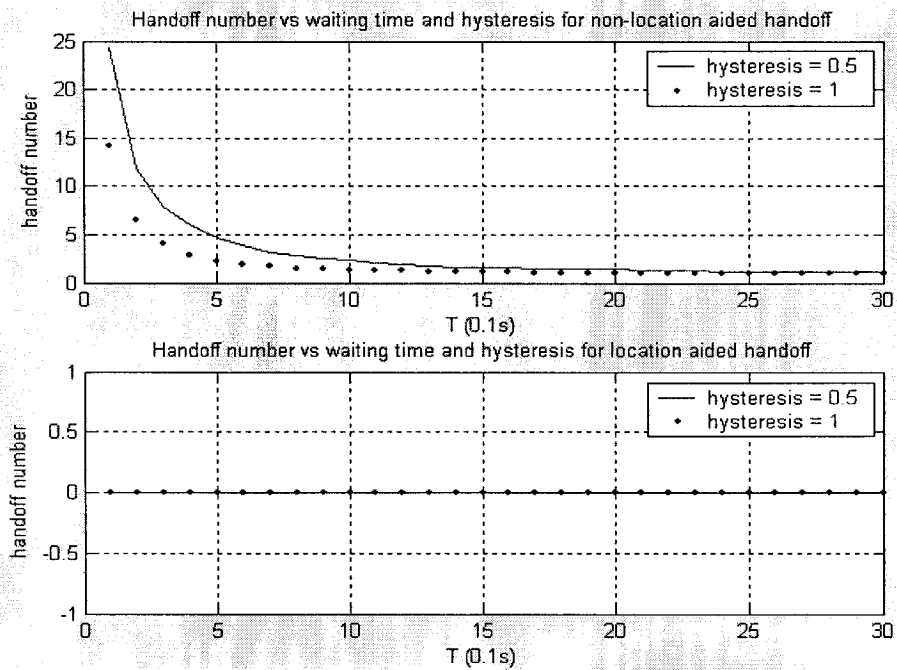


Figure 37. Number of Handoff in Transition Area

4.6.2. Battery Consumption

Scenario 3: As Figure 35 indicates, there are two paths: AB-BG and AB-BH. First we will consider road: AB-BG, and then consider road AB-BH. We set T as 2 seconds to avoid the ping-pong effect. We still assume UE speed is 1m/s. WLAN interface is always active for a non-location aided handoff. As WLAN signal strength gets strong, UE will increase battery consumption. We assume UE power consumption is 0.001w when RSS is below 10db, 0.002w when RSS reaches 10db, and 0.003w when UE detects RSS over 11db for the first time. In the location aided handoff algorithm SRNC will let UE turn on the WLAN interface 30 seconds before entering WLAN according to WLAN coverage maps, UE location, and velocity. The power consumption is 0.002w. We have added a random variable with zero mean and a variance of 15 meters, simulating the accuracy of 3G location technology. SRNC will let UE increase the frequency of signal detection at 10 second away from the WLAN area, and the power consumption will be increased to 0.003w. After moving out of the WLAN, the UE will turn off its WLAN interface for the location aided algorithm, or convert the power consumption back to 0.001w for the non-location aided algorithm. We have repeated this scenario 20 times to get an average result.

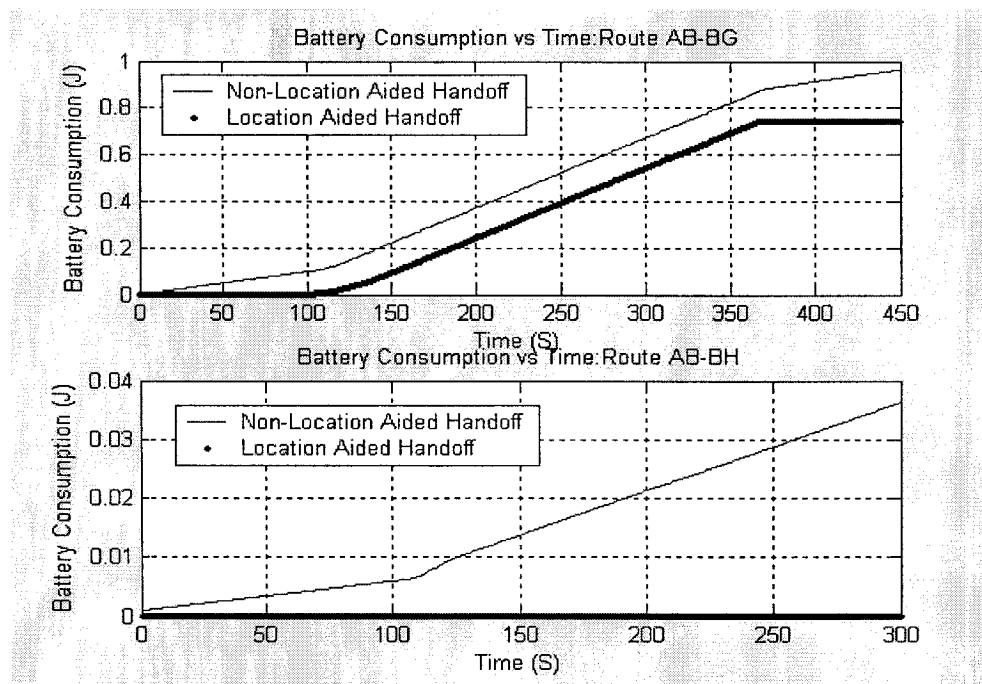


Figure 38. Battery Consumption

Figure 38 shows the battery consumption for both paths. The x coordination is time and the y coordination is the total battery consumption. The upper sub-figure is for path AB-BG and the lower sub-figure for path AB-BH. We can see that the battery consumption of the location aided handoff is much less than the non-location aided handoff.

4.6.3. Drop Call Rate and Handoff Delay

Scenario: UE moving out WLAN along road OF in Figure 35.

To make the handoff from WLAN to 3G networks the non-location aided algorithms will simply define a hysteresis(H) and waiting time(T). If the RSS is below the threshold plus H for T seconds then a handoff is supposed to launch, but during this period the connection may be dropped if RSS is less than the threshold. Also, after T, the RSS may be below threshold when UE communicates with AP for a handoff execution. It is obvious that with greater the speed, the probability of a drop call will increase. We repeated this scenario 100 times to get the average probability of drop calls at different speeds. In the location aided handoff algorithm WLAN can provide accurate location information (1 meter). SRNC will notify UE before UE reaches the WLAN boundary. The notifying time is calculated according to its speed. Therefore the drop call rate will decrease greatly. In our simulation hysteresis is assigned value 3 and waiting time is 2 second. WLAN location accuracy has been taken into consideration.

In Figure 39 the X coordinate is the UE speed; the Y coordinate of the upper sub-diagram is the probability of call drop rate, Y coordinate of the below sub-diagram is handoff delay. The upper sub-figure indicates the relationship between the drop call rate and UE speed. We can see the drop call rate is increasing dramatically as speed increases in the non-location aided handoff algorithm, while the location aided algorithm still maintains a low call drop rate. Lower sub-figure indicates the relationship between the average handoff delay and UE speed. The location-aided algorithm keeps UE connecting with WLAN for a longer time period than the non-location aided algorithm when UE speed is less than 2.5m/s. Given the same call drop rate, subscriber prefer to connecting with a higher data rate but lower cost networks. Although non-location aided handoff algorithm makes the UE connecting with WLAN a little bit longer when UE speed is

greater than 2.5m/s, the call drop rate is much higher than location aided algorithm. Therefore, location aided algorithm has better performance.

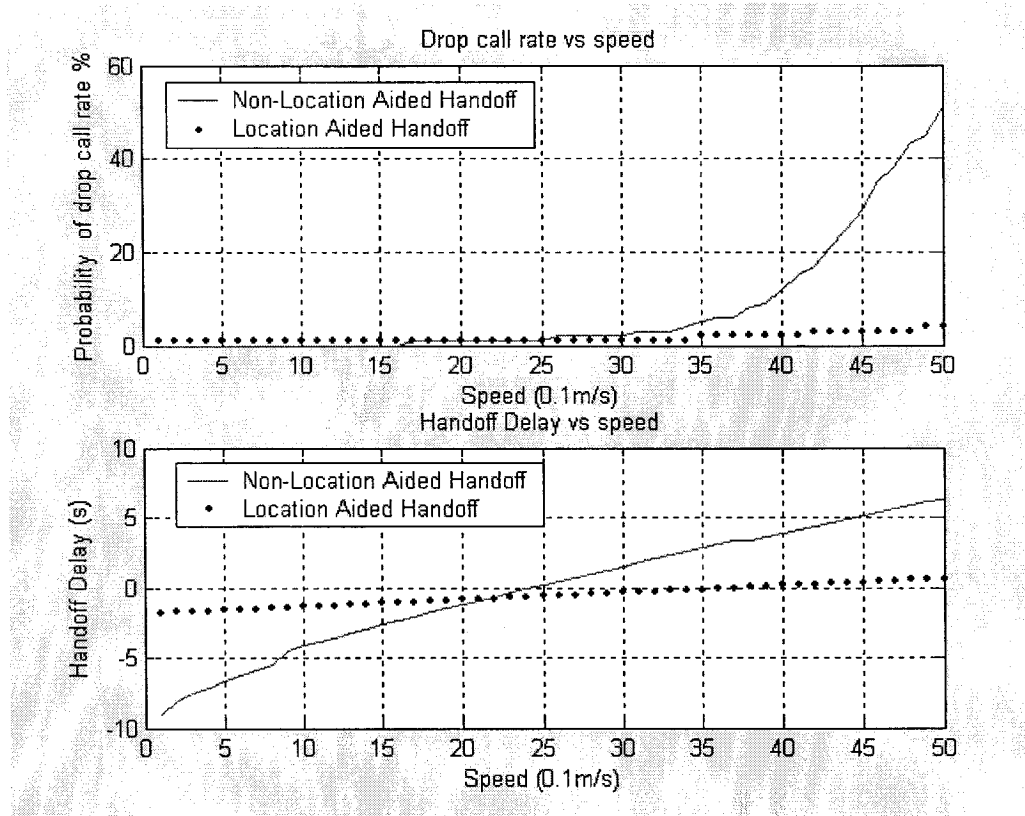


Figure 39. Drop Call Rate, Handoff Delay vs. UE Speed

4.6.4. Advantage of Road Topology

Scenario: In a WLAN there are two paths with different chosen probabilities and different lengths as Figure 34 indicated. We assume that the length of path BH in WLAN coverage is 10 meters and path BG is 100 meters. The probability that UE will walk along path BH is P , and the probability for path BG is $1-P$. If the speed of UE is v , then the dwelling time is given by $(10 \cdot P + 100 \cdot (1-P))/v$. If there is no road topology information, and UE walks along the AB, we may regard the dwelling time of UE in WLAN as $100/v$. The X coordinate in Figure 40 is the probability of path BH, the Y coordinate is the estimated dwelling time. SRNC needs to compare the dwelling time with MDT to decide if the handoff is valuable. Without road topology information, there will be a serious mistake on the estimation of dwelling time, which is used for handoff prediction by SRNC.

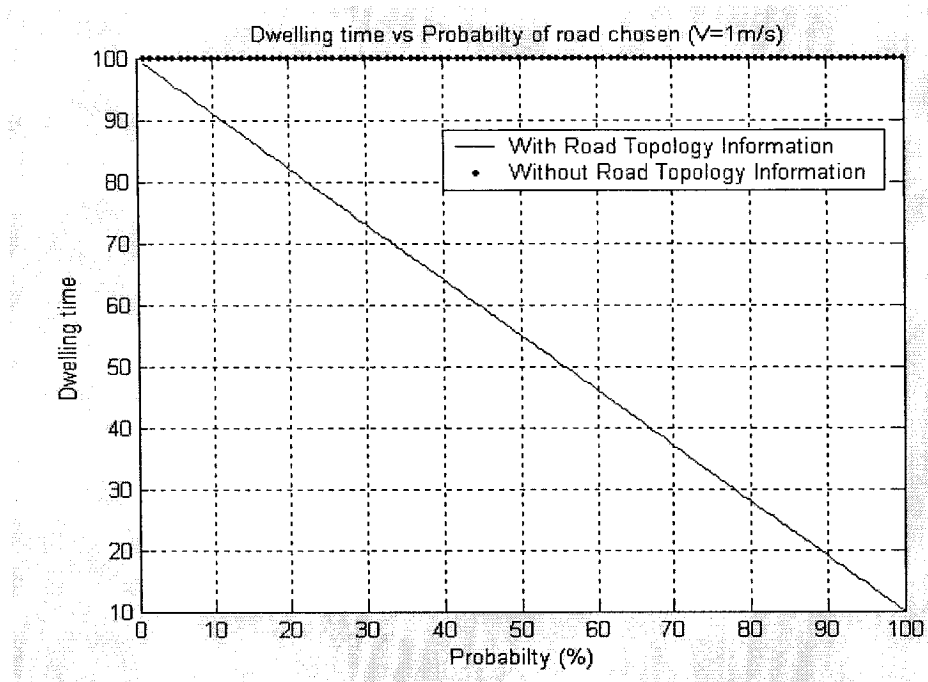


Figure 40. Advantage of the Road Topology

Chapter 5

Conclusion and Future Work

Vertical handoff is an important problem for next generation wireless networks. This thesis has presented a new architecture and algorithms for vertical handoff between 3G and WLANs. A location aided vertical handoff architecture, which takes advantage of location information provided by both 3G networks and WLAN, pedestrian topology maps, and WLAN coverage maps, is introduced. Also, algorithms to predict and evaluate the vertical handoff on SRNC side are proposed. In addition, the handoff decision strategies and signal detection algorithm for UE side are presented. Some simulations have been made to validate our approach in the areas of battery consumption, handoff delay, the number of handoffs, and call drop rates.

We can make a better evaluation on the location aided handoff solution if we have the real network and hardware environments. The velocity of UE should be considered during signal detection because it is an important factor on handoff delay. An adaptive handoff model based on velocity, RSS, and SNR should be deployed to optimize the handoff decision. In this thesis we only considered the scenarios in an outdoor environment; however, indoor environments cannot be ignored because most WLANs are confined in buildings. The inner structure of a building should be taken into consideration for handoff decision. For example, the handoff should be launched only if UE is moving towards the exit; no vertical handoff is necessary if UE is moving inside a building, regardless of its velocity and moving direction. In summary, more work is required to make it a practical solution.

Reference

- [1] M. Frodigh, S. Parkvall, C. Roobol, P. Johansson, and P. Larsson, "Future-Generation Wireless Networks", *IEEE Personal Communications*, October 2001, Vol. 8, No. 5, pp. 10-17.
- [2] T. Zahariadis and B. Doshi, "Applications And Services For The B3G/4G Era", *IEEE Wireless Communication*, October 2004, Vol. 11, No. 5, pp. 3-5.
- [3] P. Rysavy "Data capabilities: GPRS to HSDPA and Beyond", September, 2005, http://www.rysavy.com/Articles/Rysavy_Data_Paper-Sept2005.pdf
- [4] D. Pareek, "Who Will Win The Wireless Broadband Battle – WiFi, WiMax or Cellular Fixed Wireless", <http://www.wimaxtrends.com/articles/feature/f032805b.htm>
- [5] D. I. Axiotis, T. Al-Gizawi, K. Peppas, and E. N. Protonotarios, "Services in Interworking 3G and WLAN Environments", *IEEE Wireless Communication*, October 2004, Vol. 11, No. 5, pp. 14-20.
- [6] A. Doufexi, E. Tameh, A. Nix, S. Armour, A. Molina "Hotspot Wireless LAN to Enhance the Performance of 3G and Beyond Cellular Networks", *IEEE Communication Magazine*, July 2003, Vol. 4, No. 7, pp 58-65.
- [7] Q. Zhang, C. Guo, Z. Guo, and W. Zhu, "Efficient Mobility Management for Vertical Handoff between WWAN and WLAN", *IEEE Communication Magazine*, November 2003, Vol. 41, No. 11, pp. 102-108.
- [8] J. McNair and F. Zhu, "Vertical Handoffs in Fourth-Generation Multinetwork Environment", *IEEE Wireless Communication*, June, 2004, Vol. 11, No. 3, pp. 8-15.
- [9] E. Gustafsson and A. Jonsson, "Always Best Connected", *IEEE Wireless Communication*, February 2003, Vol. 10, No. 1, pp. 49-55.
- [10] M. Stemm and R. H. Katz, "Vertical handoff in wireless overlay networks", *ACM Mobile Networking (MONET), special issue on Mobile Networking in the internet*, summer 1998, pp. 335-350.
- [11] M. M. Buddhikot, G. Chandranmenon, S. Han, Y. Lee, S. Miller, and L. Salgarelli, "Design and Implementation of a WLAN/CDMA2000 Interworking Architecture", *IEEE Communication Magazine*, November 2003, Vol. 41, No. 11, pp. 90-100.
- [12] A. K. Salkintzis, "Interworking Techniques and Architecture for WLAN/3G Integration Toward 4G Mobile Data Networks", *IEEE Wireless Communication*, June 2004, Vol. 11, No. 3, pp. 50-61.
- [13] K. Ahmavaara, H. Haverinen, and R. Pichnna, "Interworking Architecture between 3GPP and WLAN Systems", *IEEE Communication Magazine*, November 2003, Vol. 41, No. 11, pp. 74-81.
- [14] S. M. Faccin, P. Lalwaney, B. Patil, "IP Multimedia Services: Analysis of Mobile IP and SIP Interactions in 3G Networks", *IEEE Communication Magazine*, January 2004, Vol. 42, No. 1, pp. 113-120.
- [15] Q. Wang and M. A. Abu-Rgheff, "Design and Evaluation of an Integrated Mobile IP and SIP Framework for Advanced Handoff Management", *IEEE Communications Society*, 2004, pp. 3921-3925.
- [16] 3GPP TS 23.234 v. 6.4.0, "3GPP Systems to Wireless Local Area Network (WLAN) Interworking; System Description (Release 6)", Mar. 2005.

- [17] K. Pahlavan, P. Krishnamurthy, A. Hatami, M. Ylianttila, J. Makela, R. Pichna, J. Vallstrom, "Handoff in hybrid mobile data networks", *IEEE personal Communication*, April 2000, Vol. 7, No. 2, pp. 34-47.
- [18] H. J. Wang, R. H. katz, and J. Giese, "Policy-Enabled handoffs Across Heterogeneous Wireless Networks", *wmsa*, p. 51, Second IEEE Workshop on Mobile Computer Systems and Applications, 1999.
- [19] F. Zhu and J. McNair, "Optimization for vertical handoff decision algorithms", *IEEE Wireless Communications and Networking Conference 2004*, pp. 867-872.
- [20] M. S. Dang and A. Prakash, D. K. Anvekar "Fuzzy Logic Based Handoff in Wireless Networks", *Proceedings of 2000 IEEE 51st Vehicular Technology Conference, (VTC2000-Spring)*, May 15-18, 2000, Tokyo, Japan, vol. 3, pp. 2375-2379.
- [21] H. Maturino-Lozoya and D. Munoz-Rodriguez, "Handoff Algorithms Based on Fuzzy Classifiers", *IEEE Transactions on Vehicular Technology*, Vol. 49, No. 6, November 2000, pp. 2286-2294.
- [22] W. Zhang, J. Jaehnert, and K. Dolzer, "Design and Evaluation of a Handoff Decision Strategy for 4th Generation Mobile Networks", *Proceedings of IEEE VTC 2003 Spring*, Jeju, Korea, Apr. 2003.
- [23] 3GPP TS23.002 V6.7.0, "Network Architecture (Release 6)", Mar. 2005.
- [24] 3GPP TS25.301 V6.2.0, "Radio Interface protocol Architecture (Release 6)", Mar. 2005
- [25] 3GPP TS25.201 V6.1.0, "Physical layer – General Description (Release 6)", Dec. 2004.
- [26] 3GPP TS23.302 V6.7.0, "Services provided by the physical layer (Release 6)", Mar. 2005.
- [27] 3GPP TS25.321 V6.4.0, "Medium Access Control (MAC) Protocol Specification (Release 6)", Mar. 2005.
- [28] 3GPP TS25.322 V6.3.0, "Radio Link Control (RLC) Protocol Specification (Release 6)", Mar. 2005.
- [29] 3GPP TS25.323 V6.1.0 "Packet Data Convergence Protocol (PDCP) specification (Release 6)", Mar. 2005.
- [30] 3GPP TS25.331 V6.6.0, "Radio Resource Control (RRC) Protocol Specification (Release 6)", Jun. 2005.
- [31] J. Laiho, A. Wacker, T. Novosad, "Radio Network Planning and Optimisation for UMTS", ISBN: 0-471-48653-1, John Wiley & Sons, 2002.
- [32] H. Holma and A. Toskala, "WCDMA for UMTS – Radio Access for Third Generation Mobile Communications", ISBN: 0471720518, John Wiley & Sons, 2000.
- [33] M. Ergen, "IEEE 802.11 Tutorial", June 2002,
http://www.eecs.berkeley.edu/~ergen/docs/mustafa_ergen_resume_LONG1.pdf
- [34] ANSI/IEEE Std. 802.11, 1999 Edition, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications", Sept. 1999.
- [35] IEEE Std. 802.11b-1999, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer Extension in the 2.4 GHz Band", Sept. 1999.
- [36] IEEE Std. 802.11a-1999, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer Extension in the 5 GHz Band", Sept. 1999.

- [37] IEEE Std. 802.11g-2003, "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Further Higher Data Rate Extension in the 2.4GHz Band", 2003
- [38] "Wireless 802.11b White Paper", VOCAL Technologies Ltd.
http://www.vocal.com/white_paper/index.html
- [39] 3GPP TS25.305 V7.0.0, "User Equipment (UE) positioning in Universal Terrestrial Radio Access Network (UTRAN), Stage 2", Jun. 2005.
- [40] S. C. Agrawal, S. Agrawal, "Location based services"
http://www.tcs.com/0_whitepapers/htdocs/atc/location_based_services_sep03.pdf
- [41] M. Chiu and M. A. Bassiouni, "predictive schemes for handoff prioritization in cellular networks based on mobile positioning", *IEEE journal on selected area in communication*, Vol. 18 NO.3 March 2000
- [42] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, and X. Gao, "A wireless LAN-based indoor positioning technology",
<http://www.research.ibm.com/journal/rd/485/xiang.html>
- [43] Y.Wang and X.Jia "An indoors wireless positioning system based on wireless local area network infrastructure" *The 6th International Symposium on satellite navigation Technology including mobile position & location service*.
- [44] M. Ademola, "Intersystem handoff for WLAN and WCDMA", Master thesis, University of Oulu, 2002
- [45] L. Nuaymi and X. Lagrange, "A Power Control Algorithm for 3G WCDMA System", <http://docenti.ing.unipi.it/ew2002/proceedings/177.pdf>
- [46] Andrea Goldsmith, "Wireless Communication", Stanford University, 2004
- [47] K. D. Wong, "Handoff Algorithm Using Pattern Recognition" Ph.D. thesis, Stanford university, June 1998
- [48] N. Tripathi, J.H. Reed and H.F. Vanlandingham, "Handoff in Cellular Systems", *IEEE personal Communication* December 1998, pp. 26-37.
- [49] Q. Zeng and P. Dharma. Agrawal, "Handoff in wireless mobile networks", *Handbook of wireless networks and mobile computing*, pp. 1-25, ISBN: 0-471-41902-8, John Wiley& Sons Inc, 2002.
- [50] N. Tripathi, "Generic Adaptive handoff Algorithms Using Fuzzy Logic and Neural Networks", Ph.D. thesis, Virginia Polytechnic Institute and State University, August 1997
- [51] 3GPP TS25.922 V6.1.0, "Radio Resource management strategies (Release 6)", May 2005.
- [52] IEEE Std. 802.11f-2003, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution System Supporting IEEE02.11 Operation", 2003
- [53] M.Ylianttila, J.Makela, K.Pahlavan, "Analysis of handoff in a location-aware vertical multi-access network", *Computer Network* 47 (2005) 185-201
- [54] Ekahau Positioning Engine™ 3.1, <http://www.ekahau.com/?id=4500>