國立台灣大學資訊管理研究所

博士論文

Department of Information Management

College of Management

National Taiwan University

Ph.D. Thesis

移動網路中合作模式的換手管理

Cooperative Handoff Management for Mobile Networks

潘育群

Yu-Chun Pan

指導教授：孫雅麗　博士

Advisor: Yeali Sun, Ph.D.

中華民國 九十八 年 一 月

Jan. 2009

移動網路中合作模式的換手管理

Cooperative Handoff Management for Mobile Networks

本論文係提交國立台灣大學資訊管理研究所
作為完成博士論文學位所需條件之一部分

研究生 ： 潘育群 撰

中華民國九十八年一月

誌 謝

博士班的學習過程終於告一段落，在這段期間中需要同時兼顧工作與研究工作，讓我在這段不算短的研究過程中，不斷的面對身心上的艱難挑戰，其中經歷了許多的挫折、徬徨，當然也有在研究過程中獲得成果所得到的成就感，所幸可以堅持下來，才有機會在今天完成自己的博士論文。

研究論文可以順利完成，特別感謝孫雅麗老師與陳孟彰老師的指導，從大學畢業之後至中研院擔任研究助理工作開始，就接受兩位老師的教誨，這當中除了專業學術上的訓練之外，收穫最大的是感受到老師在學術上對於真理追求、實事求是的態度，我將勉勵自己秉持這樣的態度，作為未來處事的準則。

另外要感謝的人很多，過去任職於中研院時的其他師長、台大計資中心林一鵬主任與網路組的同仁，感謝這些人的鼓勵支持與包容，我才有機會在工作的同時可以兼顧學術研究。在資管系 Ants 實驗室的學弟與學妹們，特別是許君與莉萍在研究工作中的輔助與建議，這些革命情感將永記於心。

還有一些好朋友，喻美、美雯、家輝、金福 與 崇龍 在這段研究過程中，傾聽我的苦衷與牢騷，最後要感謝我的父母與家人，在求學過程中默默的支持，沒有壓力只有愛與包容，讓我在工作與研究中從來不覺得孤單。要感謝的人還有很多，最後 僅將本論文 獻給所有關心我的人。

Table of Contents

List of Figures

List of Tables

中文摘要

對現今許多的網路服務提供者來說，因為多種無線網路技術的發展，在移動漫遊的環境中同時提供 WiMAX、HSDPA 與 Wi-Fi 等異質無線存取技術，讓使用者可以依據當時使用環境與應用程式頻寬上的需要，選擇不同種類的無線網路連接網際網路，這一直是網路服務提供者的遠景。在本篇論文中，我們提出了在無線網路漫遊的情境中，設計了讓許多網路服務提供者在合作模式中(cooperative)同時可以達到快速安全認證的漫遊方法與一個由使用者自己依據成本與頻寬的考量，自行決定的服務等級的方法。在無線服務提供者之間所形成的合作模式下，這些不同的無線網路技術將被整合為一個完整的資源。

要達到上述的無線漫遊網路服務目標，有四個重要的議題要在本論文探討:1)行動使用者使用 IP 之定址方式，在無線網路中移動的同時，也需要使用漫遊服務，而不受限於其無線網路服務提供者的服務區域；2)在缺乏互信的情況下，使用者與每個無線網路服務提供者之間、以及每個無線網路服務提供者之間必須建立彼此互相信任的關係，其中包含了計費、認證機制與無線資源分享；3)在漫遊時因為認證機制或者無線網路訊息交換所增加的漫遊時間，必須加以縮短，因為時間延遲對如網路電話或者串流服務的品質影響甚鉅；4)在有多個不同網路技術服務選擇下，在成本與頻寬的考量之下，使用者如何選擇其需要的無線網路技術。

在本論文中，針對計費、認證機制我們設計了讓使用者攜帶的 U-Mobile Token，此 Token 在合作模式下之不同無線網路服務提供者之間被認證，可以大幅縮短漫遊時因為認證、計費所造成的延遲。在此問題上我們也設計與實作【Fast and Secure Universal Roaming System】縮寫為 FAS-URS (唸作 Fas(t) Earth)系統，此系統證實了漫遊者在不同的無線網路服務提供者之間可以享受快速且不中斷的通訊服務。

在使用者的服務品質的議題上，目前無線網路服務提供者普遍使用單一定價(Flat-rate)，雖然使用者可以無限制使用網路資源，但是實際上卻無法保證網路服

務品質 (Quality of Service），我們也在異質無線服務業者的合作模式(例如WiMAX與 HSDPA)的環境下，提供使用者多個選項，使用者可以依據其所付出的成本與需要的服務等級，選擇最適合的無線網路服務。在我們的模擬中，其結果顯示，此架構同時提高了使用者的滿意度，也讓無線網路系統可以容納更多的使用者，創造更高的利益。在本論文中，我們延伸此服務模式至垂直換手服務，在垂直換手的情境中，除了可以達到無縫式換手之外，我們仍可保證其在原網路中之服務等級。

關鍵詞：合作模式、無縫式漫遊、無線網路、認證、計費、使用者選擇、服務模式、垂直換手、服務等級

Abstract

Employing multiple radio access technologies such as WiMAX, HSDPA and Wi-Fi in a mobile network to provide users with more cost-effective communication services has long been a vision of many service network providers. In this thesis, we propose a security roaming solution in handover scenario and provide a novel user-decided service model in a cooperative wireless network environment and in the last, we based on user-decided service model, proposed a QoS guaranteed solution in vertical handoff scenario. When the radio resources of multiple wireless networks are collectively managed, four issues are raised in such a communication environment: a) service users would like to have IP-based roaming capability as they move rather than being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region; b) the need on security and accounting management for mobile Internet; and c) the execution of AAA however would incur extra delay to handoff latency. For applications like VoIP, video streaming and TCP connections, it may disrupt the on-going communications if such latency becomes too large. d) within these versatile reless technologies, how can mobile users choose the suitable wireless network to move in. In this work, we propose an AAA-enabled roaming alliance architecture that provides fast and secure universal roaming service across multiple service domains. The associated protocols and the supporting security mechanisms are also proposed. Our design provides continuing communications service to mobile user belonging to different service operators to quickly and securely access service when roaming across multiple service domains. Mobile users only need to carry a U-Mobile Token to receive the service. The schemes proposed only incur minimal latency in security check. This is particularly important to the support of real-time mobile applications.

For the novel user-decided service model which provided with multiple service options with different levels of service quality and charges. It is up to users to choose the most suitable service option (and access network) based on their personal preference and the amount of money they are willing to pay. We use a video streaming service in a WiMAX/HSDPA network as an example to illustrate the key concepts and resource management of our approach. The results of simulation show that, under the model, the service network can accommodate more users and provide higher user satisfaction than the traditional network-decided service model. It can also achieve higher resource utilization and revenues. We also extend this service model to vertical handoff service, besides providing seamless handoff, also keep the QoS service level as in the original network.

Keywords: cooperative, roaming, AAA(auentication, authorization, accounting), user-decided, service model,vertical handoff, service level

1 Introduction

Today’s wireless networks are highly heterogeneous, with mobile devices consisting of multiple wireless network interfaces. The mobile devices roam not only between the same wireless technology but also in different wireless technologies. In the increasing complicated wireless network environment, if we want to serve user in good experience of wireless access. We should conquer many challenges to achieve this goal. Research in this area of wireless handoff management includs many dimensions as shown in Fig. 1, such as mobility protocol, security control, handoff control and QoS control . We will discuss these related issues and problem background including other researcher’s work in Chapter 2.

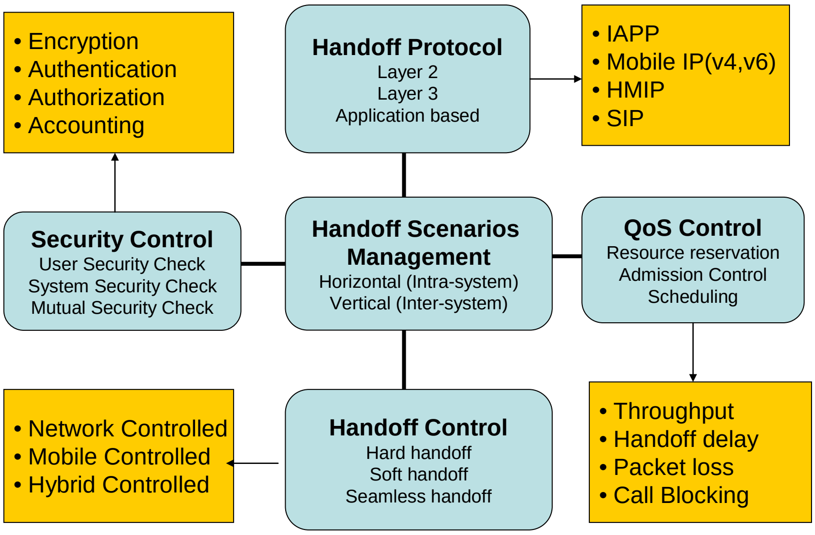


Figure 1: Research issues in handoff management

When technical details about seamless mobility and handoff across multiple administrative domains either in homogeneous network roaming scenario or heterogeneous networks, users should not need to know what wireless technology, base station, access point they are using at this given moment. Also under the condition the QoS level can be satisfied by user and maintained by operator. This thesis firstly presents the contribution in handoff security control. We propose an alliance service model called universal roaming service in which mobile users belonging to different service operators can fast and securely access needed resources provided by foreign service domains as they move without being constrained to a single spot or being forced to disconnect. In this scenario, users may access multimedia services through multi-mode mobile devices, across possibly integrated homogeneous/heterogeneous networks, anytime, anywhere they move from one cell/network to another. Secondly, we propose a novel user-decided service model to provide service option for mobile user. Under the model, when a new user submits his/her service request or the current level of service quality can no longer be sustained, the service network provider examines the resources of the individual networks, computes all possible service options, and sends the options to the user for him/her to make a choice. Each service option is described by the QoS parameters of the service application that the user requests after careful evaluation of the feasibility of using the network resources to provide the requested option and calculation of the corresponding service charge. The user then makes the final decision based on the promised service quality level and the charge information. The goal is to let service network provider conduct the resource feasibility evaluation based on the state of the cooperative network status and provide the information to the user. The final decision is made by the user, as indicated by the name of the model. Thirdly, we expend the service level option to a heterogeneous network environment in vertical handoff topic. These heterogeneous network is cooperative model, the interworking architecture can provide options to user for selection. Users take option to do vertical handoff in these networks with QoS service level guaranteed.

1.1. Problem Statement and Motivation

Because the usage of mobile wireless connection is very popular and versatile day by day, there are many wireless technologies have deployed and provided commercial service by WISP, such as WLAN, UMSS, HSDPA, and WiMAX. So it is an urgent demand to have effective method to monitor these wireless networks in good condition and serving mobile user in good feeling. This thesis focuses on finding a solution in mobility issues, including user security control and handoff QoS provisioning. We take care of these issues from three categories. The first is what kind of added value and changes to the system architecture does in network assisted or network approach bring when consider from the point of view of handoff management. Elaboration of this problem requires analysis the system architecture and related communication procedures. The second is how to utilize the different wireless technology advantage when mobile users want to make a roaming decision. Elaboration of this problem rises developing an analytical framework for handoff analysis that considers moving-in and moving-out scenarios. The goal is to find a method to provide better performance than a traditional handoff algorithm based on a received signal strength threshold. The third question is how to analyze handoff procedure in IP packet based of multimedia application. This question involves from higher application layer to lower radio interface, we need to handle the application layer QoS requirements such as service rate, delay latency in video streaming and Voice over IP(VoIP) separately and besides this, and also should looks down to mobile IP addressing overhead and underlying wireless radio network resources. The most important part but mostly will be ignored is AA(Authentication, Authorization, Accounting), AAA message exchanging is highly time expensive which will incur long latency when roaming occurs. The approach should be considered in evaluating hybrid and cross-layer analytical approach including mobile IP protocol and security relation management and also inter-domain packet-switched routing in cooperative manner.

Based on the seamless handoff requirement, the motivation to address the handoff management problem in this thesis is to develop a wireless packet-switched communication by facilitating a cooperative approach for handoff in AAA and QoS guarantee issues which can be either horizontal or vertical handoff in wireless networks. Besides the cooperative method, the consideration we take here involving the cross-layer information both in physical layer and network layer or application layers. Lower layer parameters and context information such as RSSI, CINR and location based information can be used to trigger for preparing handoff procedure. Applications and operating systems are getting more resource consuming as they are becoming more capable for supporting richer multimedia, games and other content. The whole problem area includes designing systems that can meet the requirements of mobile wireless resource managing for various applications and mobility scenarios. The most challenging task for system designers is to provide means to deliver time sensitive data such as voice or video over each mobile wireless scenario. For handoff system design, network selections have to be done between different implementation strategies for how to utilize available alternative protocols, algorithms, middleware and other technical solutions. For the end-user, it would be preferable to have suitable resource to meet the application requirement and seamless experience when roaming across multiple wireless networks.

1.2. Scope and Methodology

As was in the problem statement, the scope of problem of this thesis has three categories. Firstly, architectural issues in cooperative wireless network are discussed and a new concept of sharing alliance security information in mobile wireless network is presented. Additionally, an advance concept of user-decided service model is proposed based on the same cooperative manner. This work includes identification of the theoretical aspects around this concept and implements a prototype named FAS-URS for handoff latency analysis in AAA process for handoff management. .

Secondly, handoff efficiency is the most important issue in mobility area. We utilize the AAA alliance prototype (FAS-URS) to emulate the real roaming situation and collect the latency data to demonstrate the handoff latency reducing. In the user-decided service model work, we show many dimensions of improvement from many perspectives to prove the concept will benefit both mobile user and WISP. Thirdly, we particularly develops implementation-oriented security framework, we build the prototype of token-based security mechanism in wireless packet communications within multiple domain wireless networks. Hybrid usage of mobility management protocol for future ubiquitous Internet and networking algorithm for wireless connectivity is considered through this thesis.

1.3. Contribution of This Thesis

This thesis helps to understand the key parameters and issues in this diversity to be considered in the cooperative network interworking system design, implementation and standardization, As vertical handoff, should consider the factors that diversify the heterogeneous wireless technologies. In addition, service providers have to understand what type of applications and interworking architecture can be used in various vertical mobility scenarios. For this purpose, the process of handoff has to be elaborated, both moving in and out of wireless hotspots.

This thesis also contributes to the given research problem in AAA and a novel user-decided service model by utilizing architectural design, developing a theoretical and simulation framework and providing a proof-of-concept implementation and experimental results.

The AAA issue in handoff management is addressd in Chapter 3. The user-decided service model in heterogeneous network is presented in Chapter 4. For AAA roaming issues, in addition to architectural considerations and communication aspects, the work includes theoretical aspects around this concept and builds a framework for analysis. Results from the empirical work shows that IP layer mobility with AAA with our solution provides an efficient way to interconnect different wireless administrative domain.

The data analysis of simulation is used to illustrate the improvement of user satisfaction index and the volume of user accommodation in the cooperative network system. Most importantly is the service model also increase the revenue of wireless operator. We extend the user-decided model to vertical handoff topic. We first design a interworking architecture of WiMAX and HSDPA. This architecture besides providing the seamless (no packet loss and no handoff latency) handoff service, also guarantee the QoS service level. The simulation results show high non-disruptive service level, and user satisfaction compare to conventional lossely coupled mobile IP approach

1.4. Outline of The Thesis

The ouline of this theis is as follows. In this Chapter the importance of the studied topics for next generation networks was shortly discussed. This will be further enlightened in Chapter 2 which provides an overview of the handoff technology evolution and related works in this area, ranging from the first initial concept, and going through the current state-of-art technologies towards future B3G and 4G systems. The whole area is looked at from a system architecture design point of view to form an security alliance for holistic system architecture design including a comprehensive understanding of AAA role in roaming scenario, integration alliance model and handoff management in all IP based. A high level view for the issues related to mobility engineering, and resource and service management is provided in user-decided service work. In Chapter 3, the universal fast and secure roaming service detail is given. In Chapter 4, the original paper of novel user-decided service model is given. In Chapter 5, We based on the proposed user-decided service model, to design an operation architecure to enable seamless and QoS level guaranteed vertical handoff in WiMAX/HSDPA networks. In Chapter 6, conclusions are given in the end and including directions of future work.

2. Overview of Handoff Management and Related Works

Mobility management contains two components: location management and handoff management[1]. This Chapter gives an overview of wireless handoff management, which include homogeneous and heterogeneous handoff among the same and different wireless technologies— called horizontal and vertical handoff. Handoff management enables the network to maintain a user’s connection as the mobile terminal continues to move and change its access point to the network. As shown in Fig. 2, there are three stage processes for handoff, the first involves initiation, where either the user, a network agent, or changing network conditions identify the need for handoff. The second stage is new connection generation, where the network must find new resources for the handoff connection and perform any routing operations. The final stage is data-flow control, where the delivery of the data from the old connection path to the new connection path is maintained according to agreed-upon service guarantees. In the following discussion an overview is given for handoff management related technologies. In Fig. 3, the convergence of telecommunication and data networks has been driven by the integration of Internet technologies with wireless and cellular networks. This integration involves both radio carrier switching, network level routing information updating, and transport and application level adaption. The primary goal has been to enable these processes to appear seamless (low latency and packet loss) to the users. In addition, services provided by the operator have to adapt to the vertical mobility scenarios, and in some cases provide additional value through content-aware solutions. Service quality while switching between dissimilar system has to be managed in a systematic way.

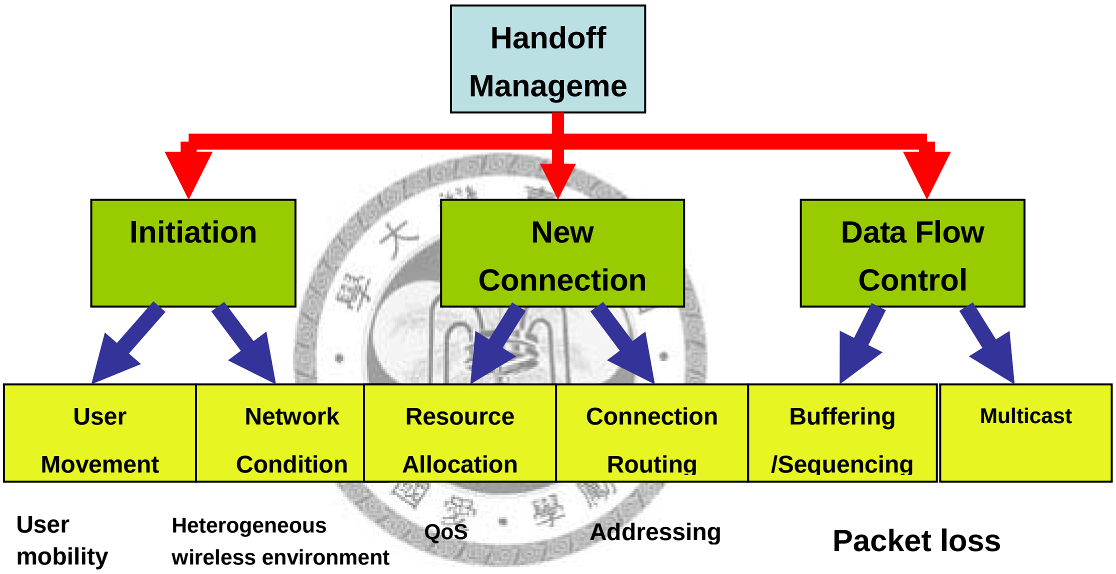


Figure 2: Handoff management operation

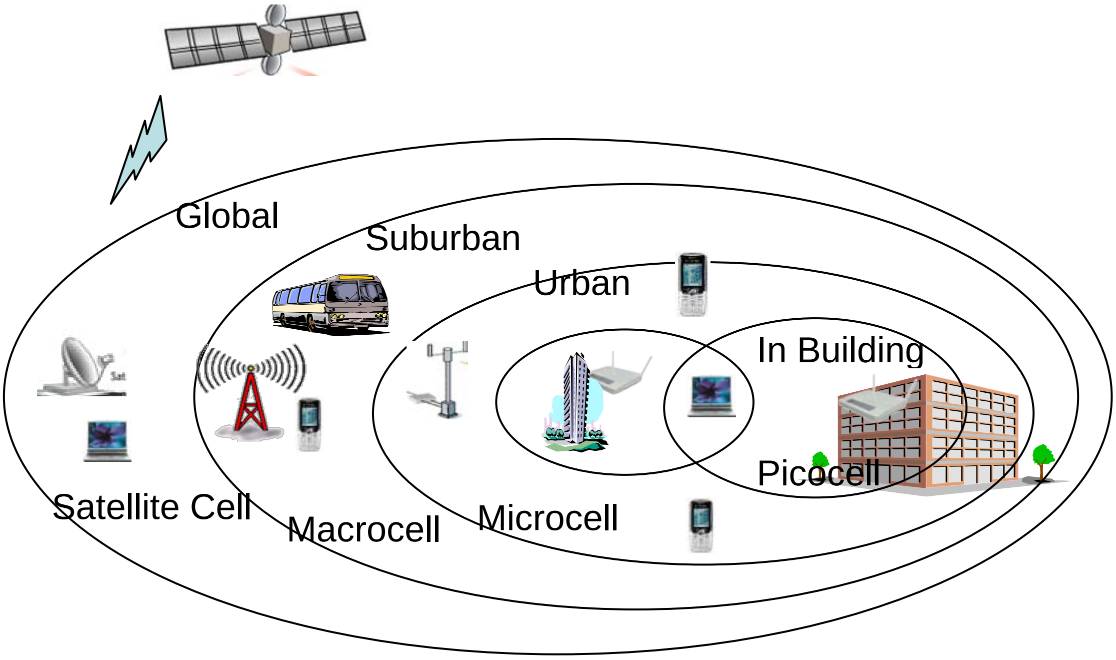


Figure 3:Next generation wireless networks

In this thesis, all the handoff technology and scenario are based on IP technolgoy. For mobility addressing issue. The Mobile IP[2] had designed for mobility purpose. Mobile IP allows transparent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from home, a mobile node is associated with a care-of address which gives information about its current location. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through a tunnel(IP-in-IP). Mobile IP provides an efficient, scalable mechanism for roaming within the Internet. Using Mobile IP, nodes may change their point-of-attachment to the Internet without changing their IP address. This allows them to maintain transport and higher-layer connections while moving. Node mobility is realized without the need to propagate host-specific routes throughout the Internet routing fabric.

2.1. Location Management

Location management enables the system to track the location of MS's between consecutive communications. It includes two major tasks. The first is location registration or location update, where the MS periodically informs the system to update relevant location databases with its up-to-date location information. The second is call delivery, where the system determines the current location of the MS based on the information available at the system databases when a communication for the MS is initiated. Two major steps are involved in call delivery: determining the serving database of the called MS and locating the visiting cell/subnet of the called MS. The latter is also called paging, where polling messages are sent to all the cells/subnets within the residing registration area of the called MS. For intersystem roaming, the design of location management techniques has the following challenges:

- ✓ Reduction of signaling overheads and latency of service delivery
- ✓ Quality of service (QoS) gurantees in different systems
- ✓ When the service area of heterogeneous wireless networks are fully overlapped:
- ✓ Through which networks an MS should perform location registrations
- ✓ In which networks and how the up-to-date user location information should

be stored

- ✓ How the exact location of an MS would be determined within a specific time constraint

The location management issue and solution are out of this thesis scope.

2.2. Horizontal handoff: Micro Mobility

Horizontal handoff includes two types of roaming situation: micro- and macro-mobility. Micro-mobility occurs when the user moves within a service area(or cell) and experiences signal strength deterioration below a certain threshold that results in the transfer of the user's call to new radio channels of appropriate strength at the same base station (BS). Macro-mobility occurs when the user moves into an adjacent cell and all of the terminal's connections must be transferred to a new BS. While performing handoff, the terminal may connect to multiple BS's simultaneously and use some form of signaling diversity to combine the multiple signals. This is called soft handoff. On the other hand, it the terminal stays connected to only one BS at a time, clearing the connection with the former BS immediately before or after establishing a connection with the target BS, then the process is referred to as hard handoff.

Handoff Management research concerns issues such as: efficient and expedient packet processing; minimizing the signaling load on the network; optimizing the route for each connection; efficient bandwidth reassignment; evaluating existing methods for standardization; and refining quality of service for wireless connections.

There are some researches in localized IP mobility management. Some requirements of this issue are (1) The mobility management signaling or binding update (BUs) caused by frequent change of CoA should be minimized (2) The Access Router (AR) should play the role of a localized mobility management agent, (3) Defining two classes of control signals for mobility management, one for inter-domain mobility and one for intra-domain mobility for MNs. The regional binding updates should employ intra-domain control signals and while the global binding updates should employ inter-domain control signals. This means that mobility management signaling should be restricted to local signaling within a domain for micro-mobility.

The primary role of micromobility protocols is t ensure that packets arriving from the Internet and addressed to mobile hosts are forwarded to the appropriate wireless access point in an efficient manner. To do this, micromobility protocols maintain a location database that maps mobile host identifiers to location information. In what follows we provide an overview of Cellular IP[3], HAWAII[4], and Hierarchical Mobile IP[3], and then present a simple taxonomy to distinguish the different mobility management approaches used to design IP micro-mobility protocols.

2.2.1. Cellular IP

Cellular IP- The Cellular IP protocol from Columbia University and Ericsson Research supports paging and a number of handoff techniques. Location management and handoff support are integrated with routing in Cellular IP access networks. To minimize control messages, regular data packets transmitted by mobile hosts are used to refresh host location information. Cellular IP uses mobile-originated data packets to maintain reverse path routes. Nodes in a Cellular IP access network monitor mobile originated packets and maintain a distributed, hop-by-hop location data base that is used to route packets to mobile hosts. Cellular IP use IP addresses to identify mobile hosts. The loss of downlink packets when a mobile host moves between access points is reduced by a set of customized handoff procedures. Cellular IP support two types of handoff scheme. Cellular IP hard handoff is based on a simple approach that trades off some packet loss in exchange for minimizing handoff signaling rather than trying to guarantee zero packet loss. Cellular IP semisoft handoff prepares handoff by proactively notifying the new access point before actual handoff. Semisoft handoff minimizes packet loss, providing improved TCP and UDP performance over hard handoff. Cellular IP also supports IP paging, and is capable of distinguishing active and idle mobile hosts. Paging systems help minimize signaling in support of better scalability and reduce the power consumption of mobile hosts. Cellular IP tracks the location of idle hosts in an approximate and efficient manner. Therefore, mobile hosts do not have to update their location after each handoff. This extends battery life and reduces air interface traffic. When packets need to be sent to an idle mobile host, the host is paged using a limited scope broadcast and in-band signaling. A mobile host become active upon reception of a paging packet and starts updating its location until it moves to an idle state again. Cellular IP access networks use special session keys where base stations independently calculate keys. This eliminates the need for signaling in support of session key management which would inevitably and additional delay to the handoff process.

2.2.2. HAWAII

The HAWAII protocol from Lucent Technologies proposes a separate routing protocol to handle intradomain mobility. Hawaii relies on Mobile IP to provide wide-area interdomain mobility. A mobile host entering a new FA domain is assigned a collocated care-off-address. The mobile node retains its care-of address unchanged while moving within the foreign domain; thus, the HA does not need to be involved unless the mobile node moves to a new domain. Nodes in a Hawaii network execute a generic IP routing protocol and maintain mobility-specific routing information as per host routes addes to legacy routing tables. In this sense Hawaii nodes can be considered enhanced IP routers, where the existing packet forwarding function is reused. Location information (i.e. mobile-specific routing entries) is created, updated and modified by explicit signaling messages sent by mobile hosts Hawaii defines four alternative path setup schemes that control handoff between access points. The appropriate path setup scheme is selected depending on the operator's priorities between eliminating packet loss, minimizing handoff latency, and maintaining packet ordering. Hawaii also uses IP multicasting to page idle mobile hosts when incoming data packets arrive at an access network and no recent routing information is available.

2.2.3. Hierarchical Mobile IP

The Hierarchical Mobile IP protocol from Ericsson and Nokia employs a hierarchy of FAs to locally handle Mobile IP registration. In this protocol mobile hosts send Mobile IP registration messages(with appropriate extensions) to update their respective location information. Registration messages establish tunnels between neighboring FAs along the path from the mobile host to a gateway FA(GFA). Packets addressed to the mobile host travel in this network of tunnels, which can be viewed as a separate routing network overlay on top of IP. The use of tunnels makes it possible to employ the protocol in an IP network that carries non-mobile traffic as well. Typically one level of hierarchy is considered where all FAs are connected to the GFA. In this case, direct tunnels connect the GFA to FAs that are located at access points. Paging extensions for Hierarchical Mobile IP are presented in [12] allowing idle mobile nodes to operate in a power saving mode while located within a paging area. The location of mobile hosts is known by HAs and is represented by paging areas. After receiving a packet addressed to a mobile host locate in a foreign network, the HA tunnels the packet to the paging FA, which then pages the mobile host to reestablish a path toward the current point of attachment. The paging system uses specific communication time slots in a paging area. This is similar to the paging channel found concept found in second-generation cellular system.

Table 1: Mapping of micro mobility protocols

	Cellular IP	HAWAII	Hierarchical MIP
Network Layer	L3	L3	L3.5
Mobile Routing Point	All CIP nodes	All routers	FAs
MN Identifier	Home address	C/o address	Home address
Intermediate nodes	L2 switches	L2 switches	L3 routers
Next MRP filed	MAC addr.	MAC addr.	IP addr.
Means of update	Data packet	Signaling message	Signaling message

2.3. Vertical Handoff

2.3.1. 3GPP Interworking Architecture

Interworking of networks especially wireless local area networks(WLANs) and UMTS(3G) is a key area of research and a great deal of efforts has been made so far. The major theme of interworking is to enable a client switch between two networks as seamless as possible without user’s intervention and maintain session mobility across different network. In Fig. 4 and 5 show that, there are mainly two architectures for interworking of WLAN with 3G, namely Thightly-Coupled and Loosely Coupled in 3GPP[5]. In Loosely-Coupled architecture a UMTS client is provided access to packet switched networks through an Interwork wireless LAN (I-WLAN) gateway under the 3G operator’s policy for authentication and authorization. The gateway connects to the Internet and has no direct connection with the 3G operator's core network. A local AAA server interacts with 3G AAA and facilitates authentication, local authorization and policy enforcement. Both of networks work independently however, network access and rights assignment is controlled by the 3G operator.

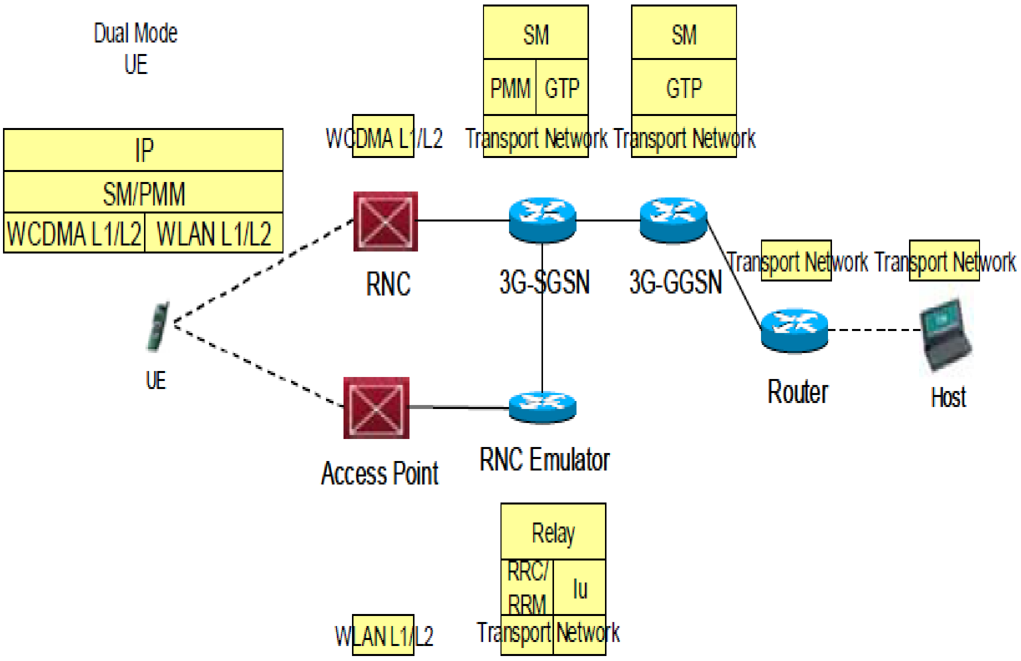


Figure 4: Tightly coupled approach

In Tightly-Coupled architecture the I-WLAN gateway is connected directly to the SGSN (Serving GPRS Support Node) of the 3G network. This means that to the 3G network, this new network appears like one of its entities with all the protocols translation taking place at the gateway node between the two networks.

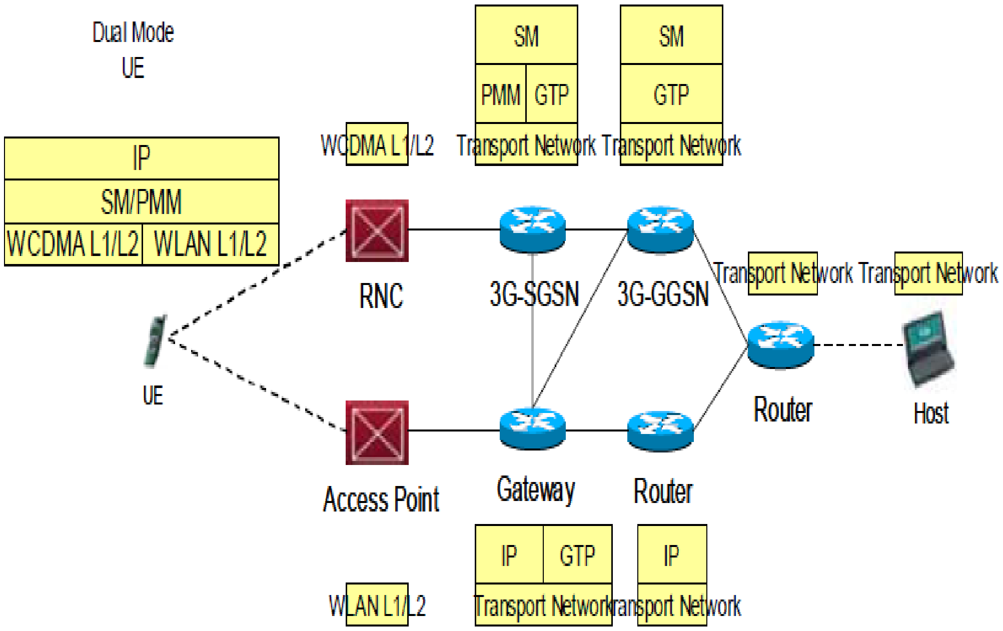


Figure 5: Loosely coupled approach

2.3.2. IEEE 802.21

It is a draft standard IEEE 802.21[6] aimed to enhance the experience of mobile users by facilitating handovers between heterogeneous networks. A framework is specified to enable service continuity when a mobile node (MN) roams between networks employing heterogeneous technologies. It specifies a media independent handover (MIH) reference model for interworking between two different link layer technologies,ref. Fig 6. An entity called the MIH Function (MIHF) is used to provide a set of handover-enabling functions within the protocol of the network elements,ref. Fig. 6.

A media independent handover Service Access Point (called the MIH_SAP). In. Fig 7, IEEE 802.21 is defined to provide MIH Users with access to the services of the

MIHF. A link layer service access point (SAP) and associated primitives is defined for each link-layer technology to allow the corresponding MIHF to collect link information and control link behavior during handovers. IEEE 802.21 identifies the functionality of framework and procedure to achieve media independent handover. However, it does not support a seamless media independent handover. It is not clear how these functional components and archtiecture be realizable in real networks in current status. Moreover, most of elements proposed by IEEE 802.21 are logical entity, and it does not define in which actual network component the specific function should be implemented.

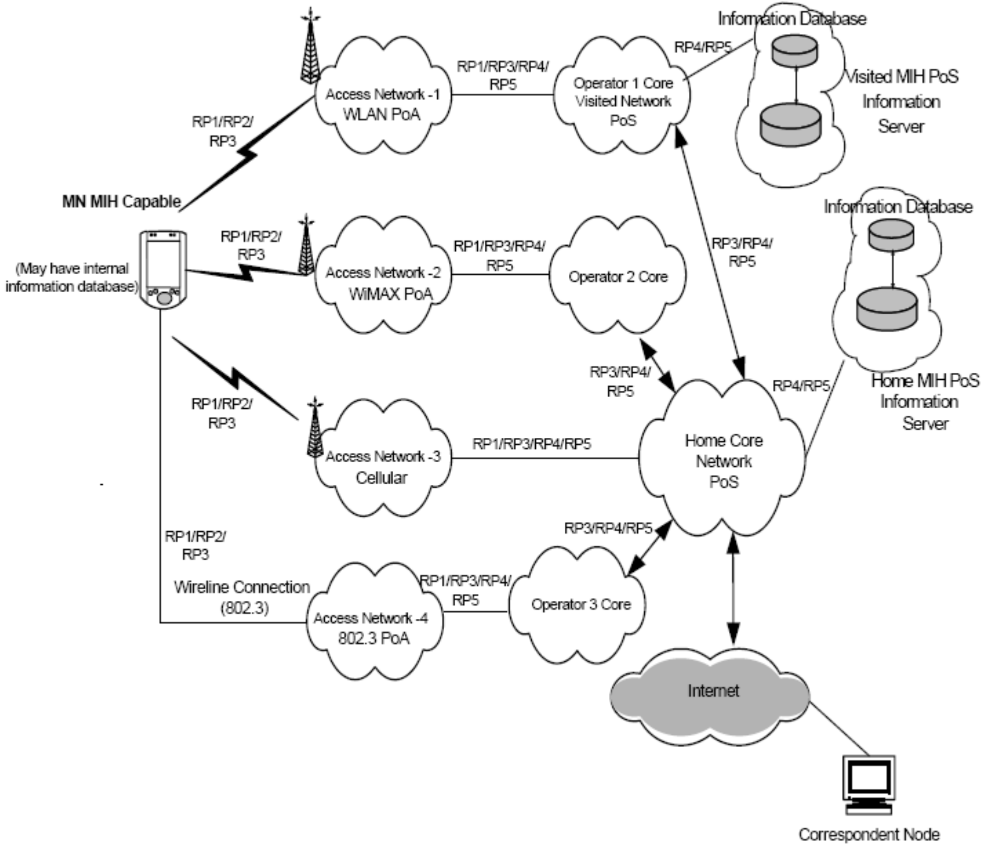


Figure 6: Example of network model with services

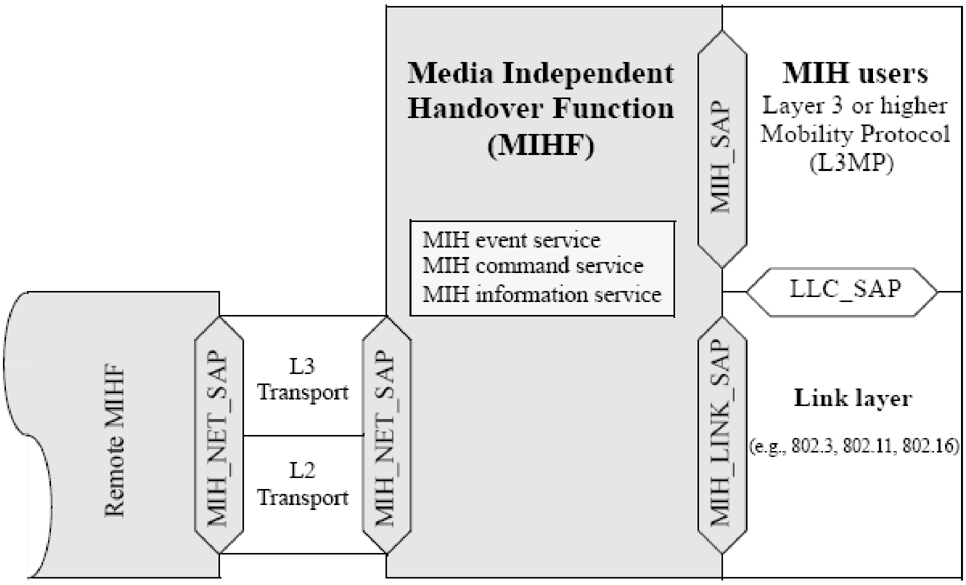


Figure 7: General MIHF reference model and SAPs

2.4. Related works

As the mention in Chapter 1 of this thesis, there are three issues in handoff management to deal with, separately they are security control, QoS control and handoff control. The following section will introduce the related research works in these topics.

2.4.1. Security Control : Mobile IP and AAA

The goal of the basic Mobile IP architecture [2] is to enable a mobile node with a registered home address in a home domain to roam across different network segments of a service domain. In the simple triangle routing model, the home agent (HA) will redirect packets destined to the mobile node to the network indicated by the mobile node’s care-of-address by using IP-in-IP tunneling technique. A more efficient communication paradigm called route optimization is to let mobile node or home agent send binding update to the correspondent node (CN).

In response to the growing demands on security and accounting management for mobile Internet, IETF has defined the AAA Framework [11][12] to assure only authenticated mobile users can get access to the resources in a foreign network. As shown in Figure 8, each network domain has at least one AAA server. A mobile node (MN) must have a home AAA and establishes a service subscription relationship with its home AAA. To receive services at a foreign domain, a MN must follow the AAA protocol for identity authentication, service level authorization and accounting for billing purpose. This AAA framework requires two security relationships established in advance: a security association (SA) between MN and its home AAA, and an SA between the foreign AAA and the MN’s home AAA.

In AAA-enabled mobile IP, there are two basic scenarios. First is that user must complete the AAA check from the service provider’s AAA server before performing Mobile IP (MIP) operations, e.g., sending the MIP registration message. The other scenario is to explore the possibility of parallelizing and/or pipelining the exchange of these messages to reduce the latency. This is important when handoff across different service domains. Figure 9 shows a simple protocol of the second approach (which is similar to the pull sequence in [12]). When a mobile node moves to a foreign domain, a mobile node sends a message containing both the Mobile IP registration request and the AAA request to the foreign agent (FA). The FA extracts the AAA request from the received message, forwards it to the local AAA server (i.e. AAAF) and waits for approval. To authenticate the foreign visitor, AAAF can either establish a security association with the mobile node's home AAA server (i.e. AAAH) or indirectly via an AAA broker. Once authenticated, the service access is enabled and FA forwards the Mobile IP registration request to HA. Note that the execution of AAA incurs extra delay to the handoff latency. For applications like VoIP [20], video streaming and TCP connections, it may disrupt the on-going communications if such latency becomes too large.

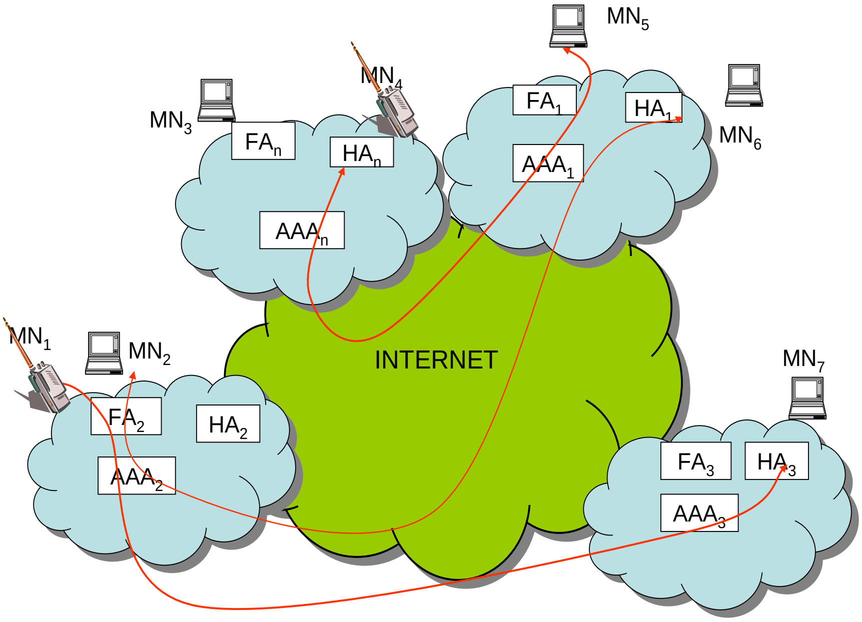


Figure 8: The mobile IP AAA turst model

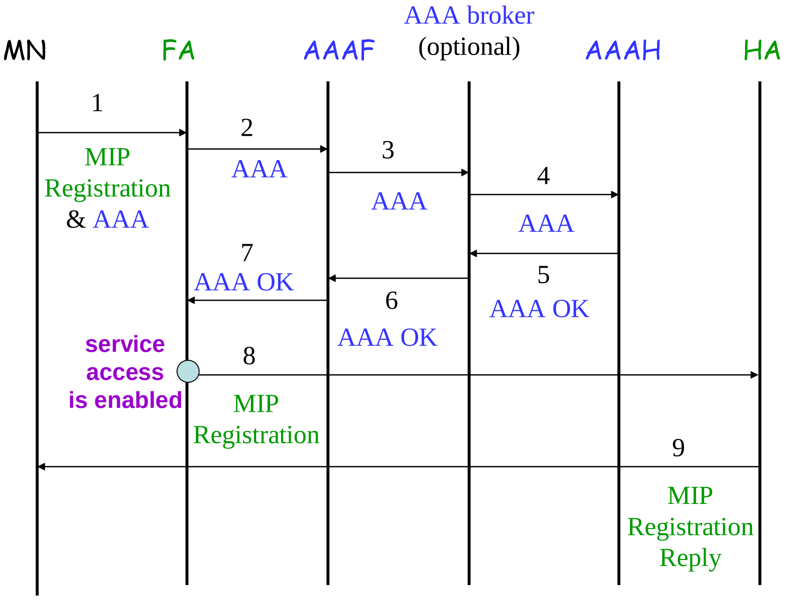


Figure 9: A simple AAA + mobile IP protocol

Although there are a number of researches on how to minimize handoff latency (such as [4][9][10]). Very few research papers addressed the fast handoff problem in secure universal roaming service. In [13], a quasi-registration method is proposed which suggests a MN's AAAH to send service authorization message to not only the requesting AAAF also some candidate neighbors of AAAF to minimize the AAA-enabled handoff latency if MN roams to these neighbor domains. However, this reference paper did not describe any security mechanisms or details about how to avoid forgery users to access the service in these neighbor domains. Neither the paper describes how AAAH would know the identities or information about AAAF's neighbors and how rigorous the authentication and authorization process is conducted between them and MN. In [14], they consider AAA with QoS requirement. They do not address roaming across multiple administrative domains.

2.4.2. QoS Control and Handoff Control : User Decided Model

A number of works focus on how to select a network to access in a heterogeneous network environment. Conventionally, the most commonly used criterion is the Received Signal Strength (RSS). In [28], the authors proposed to additionally consider network charges and the service bit rate requirement when making handover decisions between heterogeneous networks. Based on [28], [29] added more parameters to the handover criteria, including power consumption, load balance and the delay latency in vertical handover. Both works assume that handover decisions are made by the service provider networks rather than users.

In [30], a joint radio resource management scheme was proposed to reduce the call blocking probability for an 802.11 and CDMA-2000 network. The scheme requires modification of the core network structure to integrate underlying wireless technologies into one single radio access network (RAN). Again, the handover decision is made by the service provider network. The authors assume that WLAN is always the first choice for high priority data transmission. They do not consider an individual user's QoS requirement or how much the user is willing to pay as a service charge.

In [31], they used game theory to study network performance when the radio resource sharing decisions are solely made by the service users in a WiMAX/HSDPA network. In this model, resource sharing is a non-cooperative game between groups of users. The payoff function only considers the minimum throughput received per user. If any user cannot be satisfied with the goal, the network will step in to perform resource assignment. In this case, it goes back to the traditional network-decided resource assignment approach is used.

Observing that many wireless technologies are becoming increasingly popular among users, an EU research initiative called ARAGORN [32] introduced a new functional module called Cognitive Resource Manager (CRM) to help users choose a network to access in a heterogeneous wireless network environment. The CRM is responsible for collecting needed information from the network. When a user joins the environment or is about to hand off, it sends a request to CRM for network entry or a roaming decision. The decision does not consider the user's preferences for QoS and service charge. In contrast to the above works, we propose a user-decided service model for a heterogeneous wireless environment. Under the model, the service provider network evaluates all possible feasible service options in each wireless network based on the user's QoS requirements and service charge information. Decisions about network and service option selection are made by the users, who are completely aware of the QoS level choices available and the associated service charges. This model allows users to choose services according to their personal preferences and needs. We also explain how to relate application QoS requirement to the resources needed in each individual network.

2.4.3. Seamless Vertical Handoff

In [45], this is the first major paper to discuss the vertical handoff besed on IP technology, the authors specified two primary technical objectives in the design of a seamless vertical handoff system, the first issue is reducing handoff latency, the purpose is to make the switching between networks as seamless as possible for disruption-intolerant applications. The second is alleating packet loss to handoff with as little data loss as possible. However, the most important how to keep users QoS(service level agreement) was not considered in this paper or the other works in the past. In[46], the authours discussed two possible UMTS/WLAN interworking scenarios: tightly coupled and loosely coupled. They analyzed pro and con of these two interworking approaches. Ref. Fig. 4, the tightly coupled approach, firstly considering complexibility, for each WLANs operator needs to be equipped with a RNC or SGSN emulator in order to connect to the UMTS core network. The emulator is responsible for protocols translation and messages exchange between the UMTS SGSN or GGSN and WLAN AP. The additional cost of RNC or SGSN emulators may be an issue to operators. Another consideration is scalability, the WLAN and UMTS technologies are quite different. The WLAN provides high bit rate capacity (e.g. 54Mbps in 802.11g) and small coverage (e.g. 40m indoor in 802.11g) while UMTS radio access provides low bit rate capacity (384Kbps) and large coverage(1km-3km). There are different network traffic plannings for these two networks because of the differentiate network capacity. The tightly coupled approach will affect the traffic planning of network, if aggregating all traffics into one of core network. The major advantage is low handoff latency when vertical handoff occurs due to share the same FA (foreign agent), therefore no MIP procedure involved. Ref. Fig. 5, the loosely coupled approach, the advantages are no needs to be modified the component of network core device and no impacts in original traffic planning. The drawback is incurring extra MIP process with additional latency. The total latency can be broken into some parts, including scanning network, network entry, MIP and AAA process. In order to avoid the latency introuduced by MIP and AAA, In [47], based on 3GPP standard, the authors proposed a pre-authentication and -registration mechanism to facilitate fast handoff procedure. The purpose is for low latency delay, network assists mobile user in performing authentication and registration before network scanning and entry is completed.

3. Cooperative Universal Secure Handoff Service

Rapid deployment of IEEE 802.11 based wireless access networks in hot spots and the integration of the networks to the existing wide-area communication infrastructure have become a major driving force to speed up the design and development of necessary security and quality of service (QoS)-guaranteed mechanisms with roaming capacity to mobile users. Three issues are raised in such a communication environment: a) service users would like to have IP-based roaming capability as they move rather than being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region; b) the need on security and accounting management for mobile Internet; and c) the execution of AAA however would incur extra delay to handoff latency. For applications like VoIP, video streaming and TCP connections, it may disrupt the on-going communications if such latency becomes too large. In this Chapter, we propose an AAA-enabled roaming alliance architecture that provides fast and secure universal roaming service across multiple service domains. The associated protocols and the supporting security mechanisms are also proposed. Our design provides continuing communications service to mobile user belonging to different service operators to quickly and securely access service when roaming across multiple service domains. Mobile users only need to carry a U-Mobile Token to receive the service. The schemes proposed only incur minimal latency in security check. This is particularly important to the support of real-time mobile applications. We also implemented this U-Mobile Token system to measure the end-to-end latency compare to conventional AAA latency

3.1. Problem Definition

The motivation for this work comes from an observation of rapid deployment of IEEE 802.11 based hot spot wireless access networks and the integration of these networks to the existing wide-area communication infrastructures, both wired and wireless. It has become one of the major driving forces to speed up the development and deployment of new services (e.g., VoIP and multimedia content delivery) and new multi-network attachment equipment (e.g., dual-mode wi-fi/HSPA and 3G/WiMAX handset).

Our vision of the future wireless networks will have the following characteristics: *a*) different, possibly overlapping, radio access networks serving the same area; *b*) each provides different services in terms of coverage range, bandwidth or delay; and *c*) users carry small light-weight, pocket-size multi-mode terminal devices (e.g., a 3G/wi-fi/WiMAX terminal device). Users may access multimedia services through multi-mode mobile devices, across possibly integrated heterogeneous networks, anytime, anywhere they move from one cell/network to another. Network provider must develop services and applications that are able to attract customers and to produce profitable business.

To make the business model of such a vision successful, in addition to rich services catering to various subscribers' needs and tastes, we have identified one important feature for these emerging Internet services. That is the *mobility* – service users would have IP-based roaming capability as they move rather than being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region. Hence, seamless IP roaming across different service domains is an essential service to assure users good service usage experience as well as to make the service business successful. Here, a service domain is an independently administered service network. This service enables mobile users belonging to different service operators to access needed resources provided by foreign network domains. We refer to such service as the *universal roaming service*.

The importance of providing universal roaming service is easy to understand by looking at the advantage (or the success) of the current cellular phone service over the fixed-line phone service. This service model is indeed a win-win to both service providers and service users. Service providers can profit from additional use of their networks/services from the customers of other service operators. Moreover, individual operator has no need to spend enormous investment on building infrastructure that covers the entire area. All operators' investments are not overlapped and wasted due to redundancy. Resources will be better utilized. From the service user's perspective, they can enjoy convenience access to more resources whenever they go and on-going communications are guaranteed to continue. The administration issues such as service authentication, authorization and accounting should be well designed and equipped to make them transparent to service users. We believe providing universal IP roaming service is fundamental and key to the success of mobile business and mobile commerce.

One of the key factors behind the success of mobile Internet has been seamless roaming across network service borders. However, the development of universal roaming and handoff has been extremely slow so far. New technical and service provisioning challenges must be overcome. Past solutions more focus on three areas. First is the problem of roaming within an operator's own networks, e.g., HAWAII[3], IDMP[3][9]. This is no longer sufficient to meet long-term customer demands for "universal" services, anywhere and anytime. To address this goal, a number of commercial solutions have been proposed mainly in cellular phone service and wi-fi networks. They consider the problem of enabling subscribers to travel between native and foreign service areas and be able to obtain the Internet access. They expand the wider area of coverage through roaming agreement with other providers. The focus has been on addressing many of the commercial issues as they establish roaming contracts, settlement agreements, peering arrangements, and the charge for the services. For example, Vodafone and O2 have agreed to allow operators within the T-Mobile group to roam over their GPRS networks to offer some regional/national/international roaming. For a foreign operator, the issue is on the authentication check for the initial access (rather the handoff) of foreign visitors whether an access-attempt from a non-home subscriber is indeed a valid customer of an allied/trusted operator. If permitted, a foreign visitor’s roaming is treated just like an ordinary intra-domain roaming. Third, a lot of efforts from device manufacturers to provide products that enable access to voice and data services across multiple technologies and in a broad range of spectrum bands in the world for global roaming. For example, the CDMA Development Group (CDG) proposed to support seamless roaming on CDMA and GSM systems and to enable CDMA2000 customers to use their phones around the world. There are also many efforts and works mainly from the industry dedicated to the methods for wireless devices to roam across multiple cellular air interface standards and frequencies.

The goal of this work is to enable instant, seamless roaming across borders. To achieve this goal, additional intelligence must be integrated into the network so that sessions can be maintained while subscribers are roaming. This should include the security (AAA) validation so to provide continuity as subscribers roam between home/foreign, foreign/foreign service areas. The design/mechanisms must be able to separate foreign visitors' profile information necessary for service access authentication/authorization/accounting purpose from private home-network subscriber-profile information to preserve privacy while achieving universal roaming service to mobile users.

For real-time security check during handoff across borders, there must be able to provide instant access to subscriber profiles by foreign network operator so that individual requirements can be supported. Moreover, our scheme allows "home-based roaming" in which subscriber-profile information and authentication, authorization and accounting (AAA) remain on the subscriber's home network. The related service provisioning and execution are collaboratively accomplished by participating operators and across their multiple networks.

The forward-thinking operators that deploy the systems proposed here will be able to offer high-value services to subscribers wherever they go. They will flourish at the expense of competitors that stick with legacy technology.But the technical limitations of today's IP networks make it difficult for operators to share services and subscriber-profile information with other operators.

Universal seamless roaming is the ability for wireless interoperability between two or more wireless service networks. This is accomplished through rigid security support and cooperation between pariticapting operator’s networks. It requires security check control protocol, and security at customer handsets that enable the verification of three parties – the user, the home operator and the foreign operator so to ensure the accounting and no denying by user after accepting service. Moreover, such a mechanism must also address the real-time requirement during the across-service-border handoff.

There are some security works in wireless technology, we take popular 802.11i/WPA[7] as an example, the 802.11i/WPA is designed to enhance WEP security strength, use the TKIP (Temporal Key Integrity Protocol，TKIP) and longer initial vector to overcome brute-force method on WEP key attack. IEEE 802.11i/WPA method does not take care of fast roaming issue we address in this work. If MN across multiple WISP domains using 802.11i/WPA method due to AAA information should come back to home domain to complete AAA process, it will incur longer authentication time. Comparing to our work, we can securely ,quickly and smoothly accessing foreign network resource by using U-Mobile token. And the cooperative alliance concept is also proposed to provide mobile user one single bill from home operator, no matter where and when you use the network service, such as iPass[8]. The objective of security alliance is totally different from ours. The alliance function we proposed in this work, all alliance members share the authentication public key and updated alliance key periodically. The purpose is to provide fast authentication when handoff occur between alliance members.

To our knowledge, the problem of combining handoff and AAA was first addressed by us and has not been addressed in the literature. In this work, we endeavor to systematically analyze the problem and devise accurate and efficient secure and fast AAA design, schemes and algorithms.

In this work, we propose a service architecture to provide secure and fast universal handoff service across different service domains. The associated protocols and security mechanisms are also presented. The goals of our design are a) to provide continuing communications service to mobile user belonging to different service operators being able to roam across multiple service domains; b) mobile users only need to carry one single identification or service token to receive the same service on any service networks; and *c*) to minimize the handoff latency in secure (AAA-enabled) roaming service specifically to support real-time applications.

The rest of the chaper is organized as follows. In Section 3.2, we present the AAA-enabled roaming alliance architecture and the membership management protocol. The proposed model is aligned with IETF Mobile IP[2]and AAA frameworks[11][12][14]. In Section 3.3, we describe the goals and the design of

U-Mobile Token which is used to enable mobile users to fast securely roam across different service domains belonging to the same AAA roaming alliance. In Section 3.4, we present the two-stage roaming authentication procedure to achieve fast and secure handoff. In section 3.5, we give security analysis and base on the U-Mobile Token AAA approach to implement a FAS-URS(Fas(t) Earth) system and using the real system to measure end-to-end delay with our approach. Finally, the conclusion is given in Section 3.6.

3.2. Forming an AAA-enabled Roaming Alliance

In this section, we present the architecture and the protocols to form an AAA-enabled roaming alliance to support fast and secure universal roaming service. An AAA-enabled roaming alliance is an association of service domains (or service operators) that agree to cooperate with one another to expedite AAA authentication/authorization to ensure non-interrupt service to mobile users. Each alliance member supports the architecture as shown in Figure 1. They all support IP technology although individual physical networks may employ different networking technologies such as IEEE 802.11, GPRS, 3G and WiMAX. It is assumed that the AAA and mobile IP entities operating in a service domain are pre-configured to share administratively created security associations. Namely, HA and FA have established security relationships with their local AAA servers as part of the trust model in the AAA-enabled mobile IP architecture. The AAAF will dynamically establish security relationships with external authorities to check the credentials of mobile visitors and their authorized service level. The establishment of security association may use techniques such as IKE[15] and IPSec[16][17].

A roaming alliance is assumed to have a master domain, for example the creator of the alliance. The master domain is responsible for alliance membership management and the key management for the secure universal roaming service. ◦

3.2.1. Join

Member domains join the alliance by invitation from the master domain. The join process consists of two phases. In phase one, the authorities (e.g. AAA servers) of the master domain and the invited service domain authenticate each other and agree upon the keys to be used to protect the alliance service-related key distribution between them. A simple three-way handshake protocol is used (as shown in Figure 10) by exchanging the RoamAllianceInvite(), RoamAllianceAccept() and RoamAllianceAck() messages. Then they determine the four keys: transmit and receive pairs of the keys for authentication and encryption between the two AAA authorities. Here we assume the Diffie-Hellman [22] key exchange algorithm is used. If the invited domain rejects the invitation, it will reply a RoamAllianceReject() message to the master domain.

In phase two, master domain distributes the ***fast roaming authentication package*** and the ***alliance membership package*** to the newly allied domain. The former is for the new domain AAA server to distribute it to its home service users to generate U-Mobile Token. The latter is to be used by the domain AAA server to authenticate mobile users from the other allied service domains.

3.2.2. Leave

When wishing to leave the alliance, a member domain sends a RoamAllianceLeave() message to the master domain which will confirm the request by replying a RoamAllianceLeaveConfirm() message。

3.3. U-Mobile Token

Table 2: U-Mobile Token notation definition

Key **Notation**	Description
$X_{alliance}$	Alliance private key
X_{AAA}	Alliance public key
$Y_{alliance}$	Private key keep by FA/HA
Y_{AAA}	Public key sent by FA/HA in the route advertisement
HomeDomainKey	MN's home domain key
UsrPrivateKey	MN's private key
AllianceSvcKey	This key dynamically generated by two parties(AAA and MN), used for fast and secure authentication

In this section, we present the design of U-Mobile Token which is dynamically generated by mobile service users to receive secure universal roaming service. The U-Mobile token carry abundant information than traditional certification concept. U-Mobile token is dynamic generated for authentication purpose to provide more strict security protection. The benefits of the use of U-Mobile Token are two folds. First, a MN can conveniently access the subscribed service at areas or networks not owned and administered by its home domain. Second, the token is designed to enable rapid AAA check especially when roaming across multiple service domains to minimize the secure handoff latency so to avoid undesirable disruption to any on-going communications.

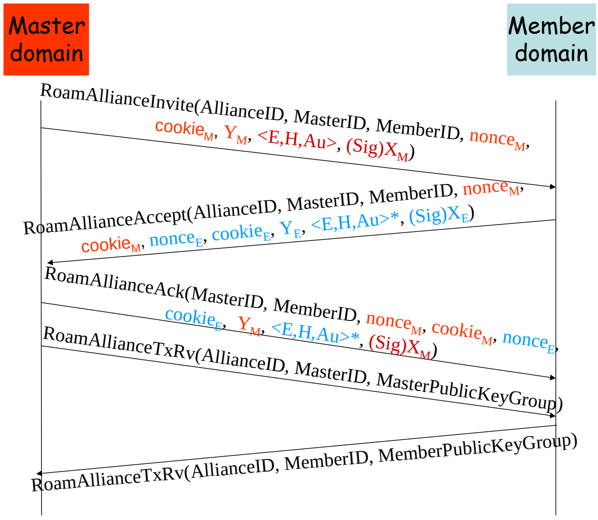

Master domain
Member domain
RoamAllianceInvite(AllianceID, MasterID, MemberID, nonce$_M$, cookie$_M$, Y$_M$, <E,H,Au>, (Sig)X$_M$)
RoamAllianceAccept(AllianceID, MasterID, MemberID, nonce$_M$, cookie$_M$, nonce$_E$, cookie$_E$, Y$_E$, <E,H,Au>*, (Sig)X$_E$)
RoamAllianceAck(MasterID, MemberID, nonce$_M$, cookie$_M$, nonce$_E$, cookie$_E$, Y$_M$, <E,H,Au>*, (Sig)X$_M$)
RoamAllianceTxRv(AllianceID, MasterID, MasterPublicKeyGroup)
RoamAllianceTxRv(AllianceID, MemberID, MemberPublicKeyGroup)

Figure 10: The three-way handshake protocol in phase one member join process

3.3.1. Design Goal

A MN subscribes the universal roaming service from a home service domain. At the subscription time, the MN will receive a fast roaming authentication package from its home AAA for the generation and management of *U-Mobile Token*. Since a wireless network is basically an open communication channel, strong authentication of mobile nodes is necessary. Under the AAA roaming architecture, a MN wishing to attach to a foreign network sends a U-Mobile Token to AAAF. For AAAF, the inspection of the U-Mobile Token should include the following three tasks:

- ✓ ***authentication of the issuing party*** **-** AAAF must check whether the received U-Mobile Token is genuine and issued by the claimed home domain.
- ✓ ***authentication of whether the token holder is truly the claimed user*** so that when AAAF issues a billing statement to the user (or user’s AAAH), user cannot deny the use of the service;
- ✓ ***integrity check*** **-** The content of the U-Mobile Token is not modified en route.

In the meantime, the U-Mobile token shall also serve the purpose of, from the mobile node’s perspective, authenticating the AAAF as a legitimate alliance member to further inspect the content of the U-Mobile Token and charge the service usage at the foreign network accordingly. These checks are necessary and important between mutually un-trusted sender (mobile user), receiver (foreign AAA) and token issuer (home domain and alliance master domain) in mobile-commerce for the purpose of service charging and billing. The service record must be undeniable and of no repudiation.

To achieve these goals, two security mechanisms are proposed: ***alliance key pair*** and ***alliance service key***.

3.3.2. Alliance Key Pair

The alliance key pair consists of a public key and a private key denoted as $Y_{alliance}$ and $X_{alliance}$. For easy reading, we summarized all used notification in Table 1. Upon joining the alliance, a member domain will receive a ***membership authentication package*** from the alliance master which contains an alliance public key $Y_{alliance}$ and two Diffie-Hellman algorithm parameters: q (a very large prime number) and α (a primitive root of q). The ***alliance private key*** $X_{alliance}$ is held by mobile service user. When a mobile user roams to a service domain (home or foreign), the AAA server and mobile node will follow a ***distributed alliance service key generation protocol*** to dynamically generate an ***alliance service key*** - a shared secret key based on the Diffie-Hellman algorithm for U-Mobile Token encryption.

The master domain is responsible for the generation of the alliance key pair according to the following equation:

$$Y_{alliance} = \alpha^{X_{alliance}} \qquad (1)$$

It is also responsible for rekeying after member join and leave. Each member AAAH will periodically receive a new alliance key pair for each service period. Here we define the service period as a valid time of Alliance key pair. The methods such as periodic batch rekeying method[18] can be used for alliance key pair management.

3.3.3. Alliance Service Key

Each mobile service user will be given a fast roaming authentication package upon service subscription time. The package contains an alliance private key $X_{Alliance}$ and the two Diffie-Hellman algorithm parameters: q and α the same as those in the alliance membership package. To secure the exchange of U-Mobile Token and for timeliness control, a ***shared alliance service key*** is devised ***between MN and AAA server (AAAF and AAAH)***. Alliance service key is dynamically generated by the two parties according to the following ***distributed key generation protocol.*** Per universal roaming service period, AAA server determines a random integer X_{AAA} as its private key and sends its public key denoted as Y_{AAA} in the route advertisement message. It then computes the alliance service key for the current service period as follows:

$$K_{allianceSvcKey} = (Y_{alliance})^{X_{AAA}} \bmod q \tag{2}$$

When received the route advertisement message, a MN computes the *current* alliance service key according to the following equation:

$$K_{allianceSvcKey} = (Y_{AAA})^{X_{alliance}} \bmod q \tag{3}$$

In this method, the shared alliance service key is never transported on the network for security. The advantages include the alliance service keys are updated and generated periodically by local AAA servers and mobile nodes (no master domain is involved); and there is no need to store alliance service keys for a long period of time for timeliness to prevent replay attack. Moreover, each service domain (even individual network segment of a service domain) may use different alliance service keys for better security control.

3.3.4. Content Design

To achieve the goals of “fast” and “secure” roaming authentication across multiple service domains of an alliance, the information necessary to carry in the U-Mobile Token is designed as follows:

U-Mobile Token = (roamAllianceID, Y_{AAA}, homeDomainID, nounce, {userID, serviceClass, homeDomainID, $\{userID\}_{homeDomainKey}$, {serviceClass, serviceLifeTime, alliancePrivateKey, allianceSvcIndex$\}_{usrPrivateKey}\}_{allianceSvcKey}$)

The roamAllianceID is the identifier of the universal roaming service alliance with which the MN’s home domain has a membership. The public key (Y_{AAA}) sent by FA/HA in the route advertisement message is repeated here for timeliness control. The homeDomainID is the identifier of the MN’s AAAH. The rest of the data is encrypted by the ***alliance service key*** generated according to the protocol in Section III.C. The purposes are three-fold. First, if AAAF/AAAH can decrypt and read the content, it simultaneously authenticates AAAF/AAAH and mobile node as a legitimate member domain and a legitimate service user. Second, the information encrypted in this data block is secure because non-allied members cannot read the content. Last, both AAAF/AAAH and MN are synchronized in terms of having the keys of the same current alliance key pair. In the case that the AAAF's (AAAH's) decryption of U-Mobile Token fails, the AAA server will forward the token to AAAH requesting for alliance private key update. The updated information from AAAH will be relayed back to the MN which can then re-compute shared alliance service key and re-issue the U-Mobile Token.

In this encrypted block, it contains three sets of data **(*info4AAA, info4AAAH*** and ***info4Update*)** related to the service. The first three fields are for AAA server's authentication of the user's access to the service (referred to as *info4AAAF*). The requested service class can be such as the gold, silver and bronze as defined in the DiffServ or detailed QoS requirements of the service user. The protected home domain id is for AAAF to forward the AAA messages. The second set of data (referred to as *info4AAAH*) is intended to forward to AAAH for token holder's identity validation, thus encrypted by AAAH's homeDomainKey. The third set of data (referred to as *info4Update*) contains four important service parameters which are intended to be forwarded to AAAH as well for information update. It is encrypted by using mobile node's private key. We assume a home AAA has access to the public keys of its service users. The allianceSvcIndex and alliancePrivateKey are the current service period index and the key used when the U-Mobile Token was sent.

3.4. Fast Roaming Authentication

The service provision to and security check of a mobile user under the proposed fast and secure universal roaming service are conducted in two stages. Decrypting a received U-Mobile Token constitutes the stage-one security check. If passed, AAA server will temporarily grant MN the requested service to keep minimal handoff latency to assure on-going communication sessions are not disrupted in handoff. The temporarily time is valid till AAAF receive reply from AAAH. While the service has started, the AAA server will continue to perform stage-two security check by sending a service authorization request message to MN's AAAH according to ***info4AAAF.*** If the authorization request is confirmed by AAAH, the service to MN will continue. Otherwise, the service will be terminated immediately. Figure 4 shows the time step diagram of the proposed scheme. The timer intervals denoted as T_a and T_b refer to the stage-one and stage-two authentication. While the former achieves faster security check, the latter keeps up rigorous security check.

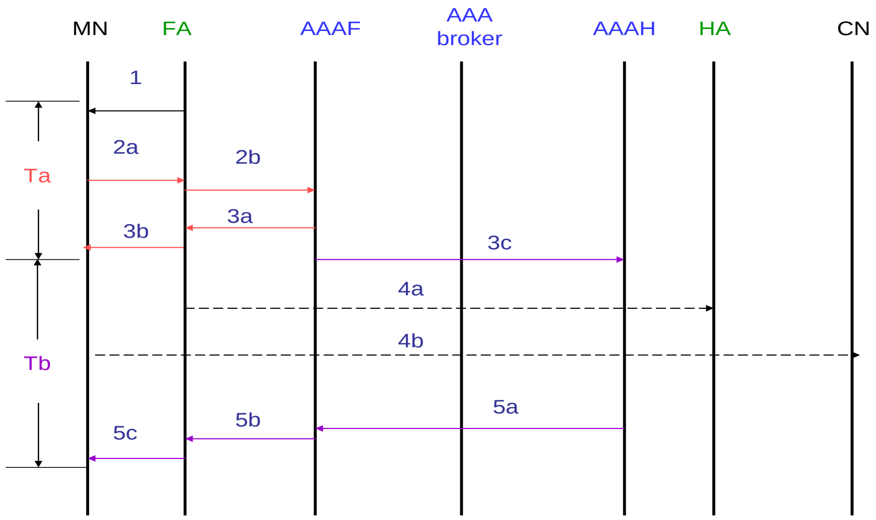


Figure 11: The protocol of the proposed fast and secure AAA enabled

Mobile IP procedure when a mobile user roams to a foreign service domain.

Message 1: FA sends a route advertisement message including $\boldsymbol{Y}_{AAA}$.

Message 2a: MN sends a message including Mobile IP registration and U-Mobile token which is encrypted by alliance service key.

Message 2b: FA forwards U-Mobile Token and forwarded it to sends the U-Mobile token to AAAF.

Message 3a: AAAF sends stage-one service authorization confirmation to FA to granting mobile user temporary service access.

Message 3b: FA replies MN a temporary service authorization.

Message 3c: AAAF sends service authorization request message to AAAH.

Message 4a: FA forwards MN’s Mobile IP registration to HA.

Message 4b: MN sends a Binding Update message to CN.

Message 5a: AAAH replies a service authorization confirmation/failure message to AAAF.

Message 5b: Depending on the service authorization result, AAAF notifies FA to either continue or terminate the service to the MN.

Message 5c: AAAF forwards the service authorization result including the information update from AAAH to MN.

3.4.1. Service Data Record(SDR)

In the *service authorization request message* to AAAH, in addition to the *info4AAAH* and *info4Update* excerpted from the U-Mobile Token, AAAF also includes its own identity and information such as a service instance identifier for complete authentication of the mobile user and authorization of the requested service. If authorization is granted, a ***service authorization confirmation message*** is sent back to AAAF. The AAAF will then notify its service equipment to continue the provisioning of the service to MN. Otherwise, a ***service authorization failure message*** is returned and the service will be terminated immediately.

The purpose of having AAAH-encrypted *info4AAH* and MN-encrypted *info4Update* are to be used as a secure proof of the service instance by MN at AAAF's service domain. Because throughput the entire course of the authentication and authorization of universal roaming service, these data are secure. No one except the home domain and the mobile node can produce, decrypt and modify the contents. As a result, the authorization confirmation will be used by both AAAF and AAAH as the *service data record* (SDR) for the service charging and billing of the home domain/mobile user.

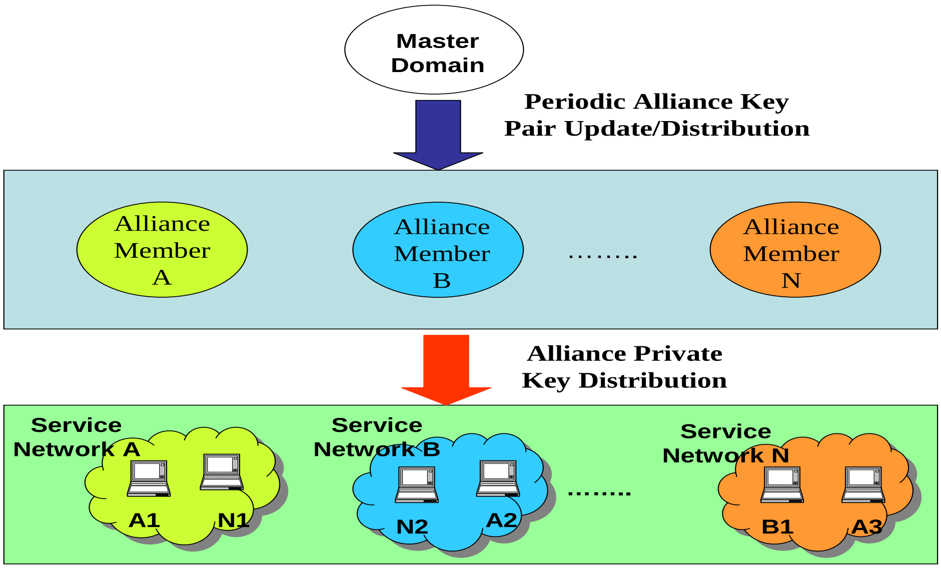


Figure 12: The alliance key pair update and distribution structure

.

3.4.2. Universal Roaming Service Management

Info4AAAH and *infor4Update* are stored in the MN's fast roaming authentication package which were originally initialized by the home AAA server at the MN's service subscription time. When received a service authorization request message, AAAH will first decrypt *Info4AAAH* to obtain user id and checks if MN is still a valid service user. If so, it then uses MN's public key to decrypt *Info4Update* and updates the content of

Info4Update with the current alliance private key, the associated service period index and the MN's service life time and service class. Here we assume when a service user subscribes the service, the value of ServieLifeTime is set to a very large number (equivalent to infinite). In the case that between two service confirmation instances the user's service subscription has been terminated, AAAH will set the ServieLifeTime to zero.

The updated *info4Update* is re-encrypted by using the MN's public key and included in the reply message (confirmation or failure) to return to MN. When received the update data, if serviceLifeTime is set to zero, the fast roaming authentication package of MN will destroy itself so that the service user will no longer be able to use the service. Otherwise, the package will update the local parameters accordingly.

3.4.3. Distribution of Alliance Private Key to Mobile Nodes

Besides the above mentioned update scenario when a mobile user issues a U-Mobile Token for service access, we still need a method to update mobile users (possibly a very large population dispersed in a very large geographic area) the new alliance private key periodically? The issues raised are not only scalability of user population, also how to locate them. There are possibilities that some users may turn off their service equipment while the home AAA is conducting the update process. The others may be in the middle of the AAA service. In the design of alliance key pair management, it is important to make sure there is no blind service period during the rekeying distribution process over a distributed environment.

The alliance key pair management is similar to group key management in terms of sharing keys among a group of users[18][19] but with higher complexity. In the universal roaming service model, three parties are involved: the master domain, member domains and mobile users. Figure 12 shows the relationship between them. The update or rekeying interval of the alliance key pair is a design parameter between the key update/distribution overheads and the degree of forward access control vulnerability. The forward access control refers to after a member leaves, it will not be able to access future communications. Here we assume the rekeying interval is the same as the service period.

In a distributed environment, it is very difficult to achieve exact synchronization of information distribution. Here, three methods are taken to synchronize the alliance key pair used by AAA server and mobile node in generating shared alliance service key. First, when a mobile user makes a first-attempt to associate to an allied network (either home or foreign) (e.g., power on the mobile equipment, “log-in” the service on a laptop, etc.), it will use the local values to generate U-Mobile Token. As described in the stage-one authentication procedure, if the MN’s alliance private key is out of date, AAAF will not be able to decrypt the token. Instead, it will forward the token to MN’s AAAH for update. After receiving the updated information, MN can re-submit the U-Mobile Token. Second, after “logging-in” the service, the MN’s fast roaming authentication package will periodically send an alliance private key update request to AAAH at the time interval aligned with the service period. Such update can be done some time right before the expiration of the service period (e.g., 1/3 of service period). Third, considering that a handoff may take place right during the period across two service periods, we introduce the notion of validation window. An AAA server will keep a window of the valid alliance key pair. We assume the window size is two. An AAAF will honor the U-Mobile Token encrypted by using either the current or the previous alliance key. It is assumed that the package residing in the MN’s equipment is secure such that the mobile user has no access to the fast roaming authentication key, thus it cannot modify the content of the U-Mobile Token such as forging a user or home domain ID.

3.5. System Implementation and Performance Evaluation

3.5.1. System Implementation

For our research work, we had implemented this system named as FAS-URS(Fas(t) Earth). We use the x86 based personal computer with Linux 2.4.7 as our development platform. Based on this hardware we installed the HIMPv6[23] to support MIPv6 and Usagi[24] Project package as development tool. In the implement process, we modified Usagi package to implement “Mobile IPv6 Fast and Secure AAA roaming” on linux kernel.

In figure 6, Mobile IPv6 FAS-URS system which include three different service domain and one mobile user(MN). The user’s home domain is Domain_NTU and may roam to foreign domains which are Domain_WIFLY and Domain_McDonald. . We use rdtsc(Read Time-Stamp Counter) which is the function provided by Pentium CPU to precisely measure Hand-off latency.

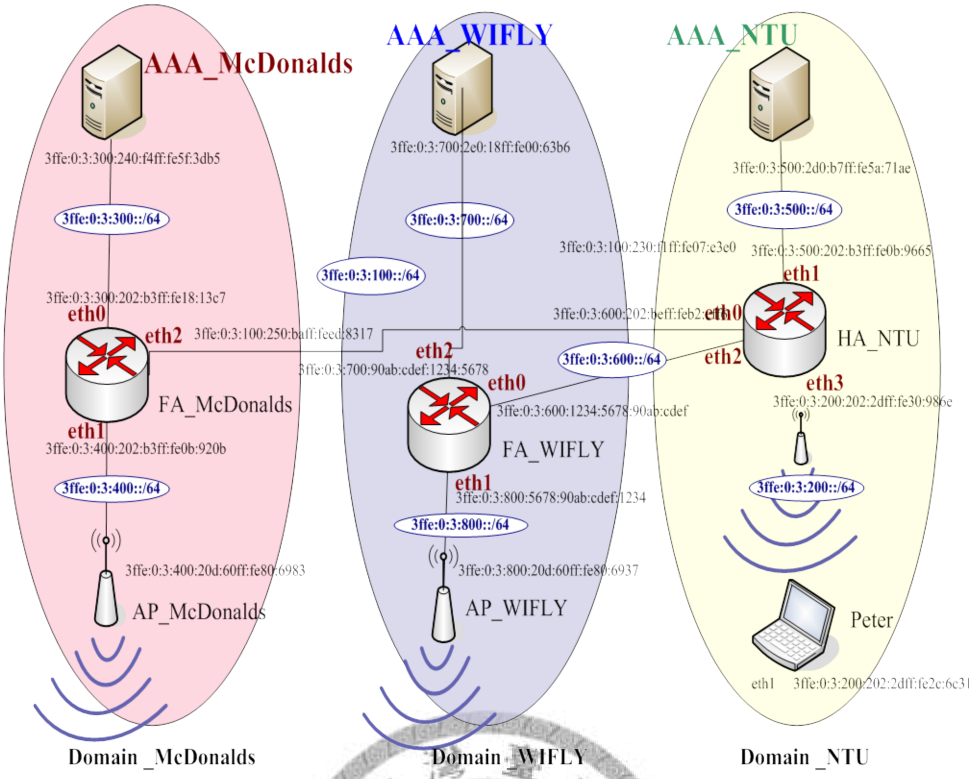

AAA_McDonalds
AAA_WIFLY
AAA_NTU
3ffe:0:3:300:240:f4ff:fe5f:3db5
3ffe:0:3:700:2e0:18ff:fe00:63b6
3ffe:0:3:500:2d0:b7ff:fe5a:71ae
3ffe:0:3:300::/64
3ffe:0:3:700::/64
3ffe:0:3:500::/64
3ffe:0:3:100::/64
3ffe:0:3:100:230:f1ff:fe07:c3e0
3ffe:0:3:500:202:b3ff:fe0b:9665
eth1
3ffe:0:3:300:202:b3ff:fe18:13c7
eth0
3ffe:0:3:600:202:beff:feb2:eth0
eth2
3ffe:0:3:100:250:baff:feed:8317
eth2
3ffe:0:3:700:90ab:cdef:1234:5678
3ffe:0:3:600::/64
eth2
HA_NTU
eth0
eth3
FA_McDonalds
3ffe:0:3:600:1234:5678:90ab:cdef
3ffe:0:3:200:202:2dff:fe30:986e
eth1
3ffe:0:3:400:202:b3ff:fe0b:920b
FA_WIFLY
3ffe:0:3:400::/64
eth1
3ffe:0:3:800:5678:90ab:cdef:1234
3ffe:0:3:200::/64
3ffe:0:3:800::/64
3ffe:0:3:400:20d:60ff:fe80:6983
3ffe:0:3:800:20d:60ff:fe80:6937
AP_McDonalds
AP_WIFLY
Peter
eth1
3ffe:0:3:200:202:2dff:fe2c:6c31
Domain _McDonalds
Domain _WIFLY
Domain _NTU

Figure 13: FAS-URS system network architecture

The system overhead which incur to MIP system is the local AAA message exchange. In Fig. 11., T**i** represent message **i** transmission latency. We have two steps process to finish AAA process. T1~T3 is the first step of AAA process and T4~T5 is the second step of AAA process.

Conventional mobile IP without AAA process, the hand-off latency time will be

T1+ T4a+T5a+T5b+T5c (4)

Our approach with secure and fast AAA hand-off process, the hand-off latency time will be

T1+T2a+T2b+T3a+T3b+T4a+T5a+T5b+T5c (5)

Since (5) – (4) the extra incurring latency will be

$$\text{AAA Overhead} = T2a + T2b + T3a + T3b \qquad (6)$$

In (6), T2a is the time which mobile user sends U-Mobile Token out to FA. T2b is the time which FA retransmits U-Mobile Token to AAAF. T3a is the time which AAAF decrypt U-Mobile Token and authenticate mobile user, after AAAF authenticated process replying temporary confirmation message (Temp OK) to FA. T3b is the time which FA retransmits confirmation message(Temp OK) to mobile user. In general network setting, mobile user, wireless AP and AAAF will be covered in the same geographic area and belong to the same wireless ISP. The data packet exchange latency between these entities is possible controlled in bounded range. AAAF decrypt U-Mobile Token overhead is light, since may use simple 3DES is secure enough. We use rdtsc (read time-stamp counter) function provided by Pentium CPU, to measure the hand-off latency in mini seconds granularity. After many times measuring, the average hand-off latency is 23.1978 ms and it is leverage in VoIP service to get higher MoS (mean of score) value.

IETF define the Inter-Domain AAA roaming service, mobile user cross network domain need to be authenticated by AAAH. In Hess's technical report[25] show that the roaming latency is dominated by packet transmitting between AAAH and AAAF. From their research results, the cross domain hand-off latency is about 52.511 ms, It's ten times the local intra-domain hand-off latency. With our approach, we can minimize hand-off latency to provide better qualitative hand-off service.

3.5.2. Security Analysis

Wireless security faces a number of threats. The major aspects of security are authentication, cryptography and attack-in-the-middle[26][27]. Addressing to the authentication problem, we use the PKI(public-key-infrastructure) to derive the allianceSvcKey key to authenticate the mobile user belong to the alliance. In the process of creating allianceSvcKey, which need to exchange local AAA and alliance public key first, in this procedure the mobile user and operator had mutual authentication each other. The allianceSvcKey key is used to encrypt the U-Mobile token and keep token privacy. Because of this session key is generated locally and will dynamically updated due to alliance public key($Y_{alliance}$) periodically renewed by Alliance master domain. By this way, we also avoid the man-in-the-middle attack; because of man-in-the-middle attack can only be successful when the attacker can impersonate each endpoint to the satisfaction of the other. In the fast authentication scenario we design here, there is no way to have fake user or operator within the authentication process. We also include nonce in the token to prevent replay attack.

3.6. Summary of This Work

In this work, we first propose a service model called universal roaming service in which mobile users belonging to different service operators can fast and securely access needed resources provided by foreign service domains as they move without being constrained to a single spot or being forced to disconnect because his/her service provider does not have entire coverage of the city/region. Due to this situation, there are two issues need to be taken care. First, AAA issues are not only to deal with single sign-on to pass user authentication. Second, we need to shorten the authentication process time. In this Chapter, we address these two important issues and then propose the architecture and the protocols to form an AAA-enabled roaming alliance to allow different service operators to cooperate with one another to expedite AAA authentication/authorization to ensure non-interrupt service to mobile users. The supporting security protocols and algorithms including the generation and management of the alliance key pair and the alliance service key for U-Mobile Token are described. Our design of U-Mobile Token successfully achieves the authentication of the issuing party and the holder as well as the integrity of U-Mobile Token by AAA servers (AAAF and AAAH), and the authentication of AAA server as a legitimate service authority by mobile node. The schemes support undeniable and of no repudiation service data records for service charging and billing. This is necessary and important between mutually un-trusted mobile user, foreign AAA and token issuer (home domain and alliance master domain) in mobile-commerce. Moreover, the U-Mobile Token is so designed to facilitate two-stage security check for not only rapid service provision to mobile user with minimal handoff latency, also with strong, rigorous service authentication and authorization.

Our design of the fast and secure universal roaming capability to mobile users which we believe is an essential feature both to provide users good service usage experience and to make the service successfully. This is fundamental and key to the success of mobile business and mobile commerce.

Base on the design, we implement FAS-URS(Fas(t) Earth) system to demonstrate the efficiency of roaming within different WISP. People can get good experience in wireless service.

4. Cooperative User-decided Service Model

Employing multiple radio access technologies such as WiMAX, HSDPA and Wi-Fi in a mobile network to provide users with more cost-effective communication services has long been a vision of many service network providers. In this chaper, we propose a novel user-decided service model for a cooperative wireless network in which the radio resources of multiple wireless networks are collectively managed. Under the model, users are provided with multiple service options with different levels of service quality and charges. It is up to users to choose the most suitable service option (and access network) based on their personal preference and the amount of money they are willing to pay. We use a video streaming service in a WiMAX/HSDPA network as an example to illustrate the key concepts and resource management of our approach. The results of simulation show that, under the model, the service network can accommodate more users and provide higher user satisfaction than the traditional network-decided service model. It can also achieve higher resource utilization and revenues. This demonstrates the importance of defining the concept of user-decided service model in a cooperative heterogeneous networking environment.

4.1. Problem Definition

It has long been a vision of broadband wireless network operators around the world to evolve their mobile networks to support multiple access technologies, such as WiMAX, HSDPA (High Speed Data Packet Access) and Wi-Fi. The goal is to take advantage of these powerful wireless technologies to provide users with convenient, pervasive and cost-effective communication services. This raises two issues. First, for service network providers, it is important that the multiple radio access technologies be collectively managed in terms of service provision. Second, there is some debate about whether the decision regarding which access network to choose would be best made by the network or whether it should be the user's choice. In the past, the service decision model was simple: user might submit his/her QoS requirement, and it was up to the network to make the final decision based on its evaluation of the state of the network and resource usage. Usually the decision would be the one that best suited the service network provider's business goal.

In this work, we propose a novel user-decided service model for cooperative wireless networks in which multiple radio access technologies are employed and the radio resources are collectively managed. Under the model, when a new user submits his/her service request or the current level of service quality can no longer be sustained, the service network provider examines the resources of the individual networks, computes all possible service options, and sends the options to the user for him/her to make a choice. Each service option is described by the QoS parameters of the service application that the user requests after careful evaluation of the feasibility of using the network resources to provide the requested option and calculation of the corresponding service charge. The user then makes the final decision based on the promised service quality level and the charge information. The goal is to let service network provider conduct the resource feasibility evaluation based on the state of the cooperative network and provide the information to the user. The final decision is made by the user, as indicated by the name of the model.

The user-decided service model offers several benefits. First, the service network provider can ensure higher user satisfaction when provisioning services in a multi-networking technology service environment. This is because users can make service selections according to their preferences as well as their concerns about quality of service and acceptable prices rather than the service provider network making the decision for them. Second, each radio technology has different transmission characteristics in terms of network capacity scale and service rate plan. The results of simulation show that, by considering users’ preferences, a cooperative network has the flexibility to accommodate more users and achieve higher resource utilization and revenue.

In this work, we use a real H.264 video streaming service in a WiMAX/HSDPA network to demonstrate the feasibility of the proposed service model. We also explain how to relate application QoS requirement to the resources needed in each individual network.

The remainder of the work is organized as follows. In Section 4.2, we detail the service quality specification of the H.264 video streaming service. In Section 4.3, we present an overview of the network resource requirements in WiMAX and HSDPA in terms of the transmission bit rate based on the H.264 quality level and the user station's channel condition. Our subjective is to show how to link the application-level QoS requirements to the lower-layer resource management in order to support the user-decided service model. In Section 4.4, we describe three important elements in user-decided service model: service charge, evaluation of user satisfaction and channel access scheduling to guarantee application's QoS requirements. In Section 4.5, we present the simulation results of the number of users admitted, network resource utilization, user satisfaction and the revenue using the proposed user-decided service model, and its comparison with traditional network-decided service model. Then, in Section 4.6, we summarize our conclusions.

4.2. Application Service: Video

Streaming

We take video streaming as an example of an application service to illustrate the proposed user-decided service model. H.264 is chosen as the codec technology for the service. It employs layered coding and can support robust delivery of a broad range of applications in a wide variety of networks and channel-type environments, ranging from very low bit rate, low frame rate, and low resolution for mobile devices to high bit rate and high resolution HDTV.

Table 3: Different video quality levels of H.264

Video Quality Level number	Max/Min bit rate (r_{max}/r_{min})
2	2048/768kbit/s
1.3	768/384kbit/s
1.2	384/192kbit/s
1.1	192/128kbit/s
1b	128/64kbit/s
1	<=64kbit/s~

To enable multi-vendor end devices to successfully interwork with each other, all H.264 encoders and decoders (software and hardware) must conform to the standard specification. H.264 defines the profiles and levels to achieve such conformance and interoperability. A profile specifies a particular set of coding function requirements for an encoder and decoder. For example, the Baseline Profile supports intra and inter-coding (using I- and P-slices) and is suitable for applications like video telephony. The Main Profile supports interlaced video and inter-coding using B-slices and is suitable for applications like television broadcasting. Additionally, the Extended Profile specifies modes for efficient switching between coded bit streams and improving error resilience. It is useful for streaming media applications. A level is defined to place limits on the parameters, such as the sample processing rate, picture size and coded bit rate of user devices. The first two parameters are related to the performance of user devices, and the third specifies the network QoS requirements. Sixteen levels from 1 to 5.1 have been defined in H.264/AVC [33] with the maximum bit rate ranging from 64kbps to 240Mbps. For the current 3G and WiMAX networking environments, six level numbers are considered here as listed in TABLE 3. A H.264 video streaming service request must specify the requested level number.

4.3. Network Resource-Application View

We now present the network resources in the term of the QoS parameters defined for each network type from an application (or service) viewpoint, i.e., the Network Resource-Application view. These are the resources that a WISP can leverage to provide users the possible service options.

4.3.1. WiMAX Resource Management: OFDMA Symbol Scheduling

Here, we consider a WiMAX network based on the IEEE 802.16-e 2005 standards. It provides mobile broadband wireless services with the geographical coverage scale of a metropolitan area. In WiMAX, the physical layer technology is based on Orthogonal Frequency Division Multiple Access (OFDMA) [34]. In the MAC layer, WiMAX frames are constructed in two dimensions: subchannels in the frequency domain and OFDMA symbols (or time slots) in the time domain. User data are carried in areas called bursts, each consisting of a group of subchannels and associated OFDMA symbols (see Fig. 14). Data carried in the same burst are coded using the same coding and modulation, randomization, FEC coding and bit interleaving techniques.

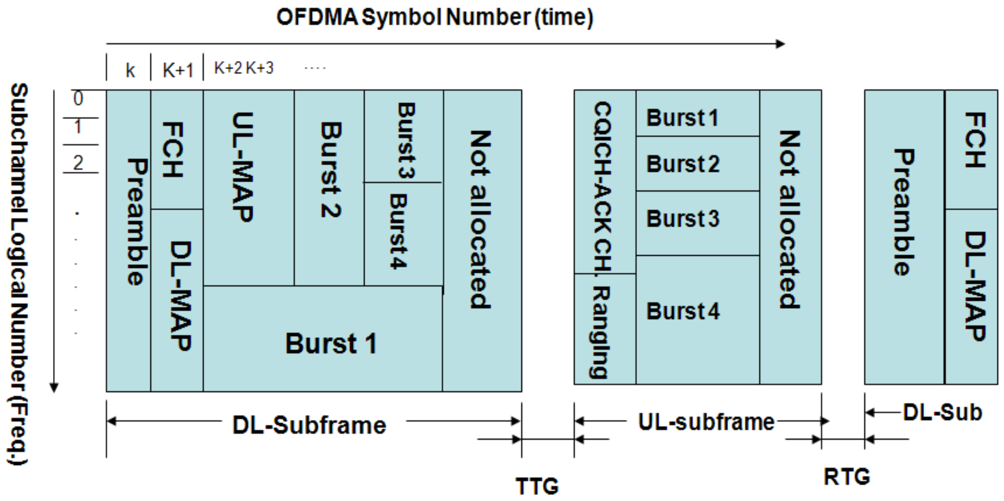


Figure 14: The WiMAX frame structure

In WiMAX, the radio transmission quality is measured by CINR (Carrier to

Interference plus noise ratio). The better the channel quality, the larger the amount of data that can be transmitted using a higher modulation method (e.g., 64QAM (3/4)), and the smaller the number of OFDMA symbols with more data bytes per symbol. Seven modulation options are specified in the standard, as shown in TABLE 4. Each mode carries a different amount of data per time slot and requires a different maximum number of concatenated time slots to carry a certain amount of data.

A H.264 video streaming service request specifies its video level number requirement *l* to the WiMAX network. According to the transmission rate range of the desired video quality level number and the channel condition of the user's mobile station, the WiMAX network resource management system examines the state of the network and computes the set of feasible transmission modes for user's selection. Each mode specifies the bandwidth allocation, service fee and discount rate.

Table 4: The modes of channel coding and modulation in WiMAX

Mode (k)	Modulation	Useful data per slot (B_k)	Max number of concatenated slots	Max data payload
0	QPSK(1/2)	6 bytes	6	36 bytes
1	QPSK(2/3)	9 bytes	4	36 bytes
2	16QAM(1/2)	12 bytes	3	36 bytes

3	16QAM(3/4)	18 bytes	2	36 bytes
4	64QAM(1/2)	18 bytes	2	36 bytes
5	64QAM(2/3)	24 bytes	1	24 bytes
6	64QAM(3/4)	27 bytes	1	27 bytes

For a service instance *i*, given the required service level number and its channel condition, we have the bandwidth *r* (bps) allocated for mode *k* as follows:

$$r_i(WiMAX, k) = B_k \times \sum_{j=1}^{b_i} (f_j \times m_j) \times F \tag{7}$$

where B_k is the useful data per slotl of mode k; b_i is the number of bursts allocated to instance *i*; f_j and m_j are the number of subchannels and the symbols allocated to a burst *j*; and *F* is the number of frames per second. In addition,

$$r^l_{\min} \le r_i(WiMAX, k) \le r^l_{\max} \tag{8}$$

Variables $\tilde{f}$, $\tilde{m}$ and $\tilde{b}$ are parameters controlled by the WiMAX resource manager. The information about which coding and modulation methods to use on allocated bursts is carried in UL-MAP (UpLink) and DL-MAP (DownLink) of each frame to the mobile stations (MS). Each MS will follow the information for its data receiving and sending.

4.3.2. Resource Management in HSDPA

There are two types of downlink transport channels for data transmission in

HSDPA: the downlink Dedicated Channel (DCH) which is a resource reserved for each service user; and the High Speed Downlink Shared Channel (HS-DSCH), which is a common channel shared between users in a cell [35]. Hence, a user may be allocated resources in both types of channel. When a channel is assigned, it is configured with a spreading code; and each spreading code is associated with a spreading factor (SF). The SF allocation is based on the Orthogonal Variable Spreading Factor (OVSF) code tree. The value of SF determines the bit rate of a channel.

The OVSF code tree is a binary tree, as depicted in Fig. 15. The HSDPA downlink resource manager uses it for resource allocation. The SF value of a node depends on its position in the tree. For the downlink transmission, the value of SF ranges from 4 to 512. To ensure orthogonality, when a code is assigned to a node, its parent and child nodes are blocked from use. This ensures that all assigned spreading codes can be used at the same time.

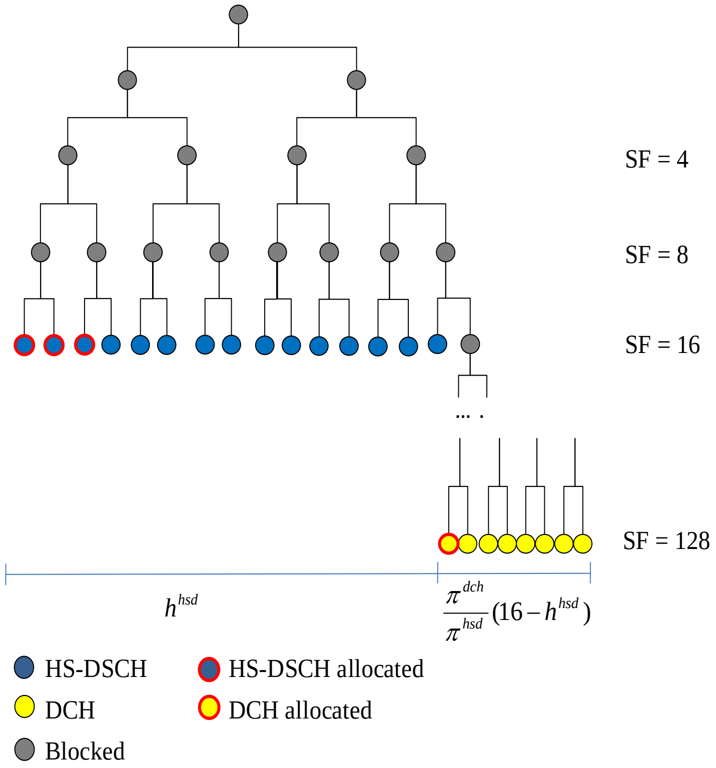


Figure 15: The spreading factor allocation in the OVSF code tree

The current HSDPA standard sets the SF value of HS-DSCH, denoted by π^{hsd}, to 16. The value of SF, denoted by π^{dch}, of a DCH is set by the system. Once determined, all DCH channels will have the same SF value which does not vary from frame to frame. Moreover, it is up to the network resource manager to decide the numbers of channels reserved for HS-DSCH and DCH. The standard sets a maximum number of spreading codes for HS-DSCH, $h^{hsd}{}_{max}$ to 15. Let the number of channels assigned to HS-DSCH and DCH be denoted by h^{hsd} and h^{dch}, respectively. We calculate the total number of DCH channels as follows:

$$h^{dch} = \frac{\pi^{dch}}{\pi^{hsd}}(16-h^{hsd}) \tag{9}$$

Let C^{HSDPA} denote the capacity of a HSDPA downlink channel. The bit rates of a

HS-DSCH and a DCH channel, denoted by r^{dch} and r^{hsd} , as follows:

$$r^{hsd} = \frac{C^{HSDPA}}{\pi^{hsd}} \quad \text{and} \quad r^{dch} = \frac{C^{HSDPA}}{\pi^{dch}} \tag{10}$$

The individual total capacities of the HS-DSCH and DCH channels are as follows:

$$C^{hsd} = \frac{C^{HSDPA}}{\pi^{hsd}} h^{hsd} \quad \text{and} \quad C^{dch} = \frac{C^{HSDPA}}{\pi^{dch}} h^{dch} \tag{11}$$

In HSDPA, each service request is allocated one DCH channel and zero or more HS-DSCH channels based on the bandwidth requirement of the requested service level number, i.e.,

$$r_i(HSDPA,k) = r_i^{dch} + n_i r_i^{hsd} \tag{12}$$

where n_i is the number of HS-DSCH channels allocated to the service instance i. This variable is controlled by the HSDPA resource manager such that

$$r^l_{\min} \le r_i(HSDPA,k) \le r^l_{\max} \tag{13}$$

4.4. The User–Decided Service Model

The concept behind the user-decided service model is that the service provider network evaluates all possible service options based on the state of the cooperative network it manages and provides the information together with the service rates to the users. A user then chooses the service level and network that best suits his/her needs and the amount of service charges he/she can accept. The model considers the quality of service that the user requests, and allows him/her to consider the service charges when selecting a service.

4.4.1. Service Charge

Table 5: The service rates for the levels of H.264 video streaming service

H.264 level number	WiMAX service fee	HSDPA service fee
2	80	100
1.3	64	80
1.2	52	65
1.1	48	60
1b	44	55
1	40	50

Each service option provided is described by two elements, the QoS level (e.g., the H.264 level number l) and service rate (and in which network type). TABLE 5 shows the service rates for the six quality levels of H.264 video streaming service in the WiMAX and HSDPA networks. We have set the service rates in WiMAX cheaper than those in HSDPA based on the ADSL rate plans of NTT [36] and CHT [37]. Because no WiMAX service is currently provisioned, we consider that similar to ADSL WiMAX technology is aimed for the last mile broadband access service solution. We compare the existing service rates of ADSL and 3G and therefore set the WiMAX service rates to 80% of those of HSDPA.

4.4.2. User Satisfaction

To evaluate user satisfaction under the proposed user-decided service model, a user satisfaction function is designed to measure whether the collectivities of the service meet user's goals [38][39]. A general approach to construct user satisfaction function is to collect real user feedback data and then perform positive correlation of the data to define the function with multiple dimensions; each may be assigned with a different weight [40]. Here, we consider two dimensions in defining the user satisfaction function: the user-perceived QoS and the service charge.

Wireless networks are constructed following the open system interconnection (OSI) layered structure where each layer performs a distinct role and has the potential to impact upon the performance of the layers above it. At the application layer, a user-perceived QoS may be poor due to network congestion and packet loss in the network layer. In turn, it may be resulted from improper bandwidth sharing and allocation at the MAC layer. Meantime, each layer protocol defines its own QoS parameters and may use different methods for resource management. Taking all layers of QoS parameters in the modeling of user-perceived QoS is too complex and not realistic. In this work, we consider the actual bit rate received in delivering the contents is the most important QoS parameter that affects the viewing experience of video streaming service to the users. Hence, it is used to measure user-perceived QoS.

In [41], a subjective survey of user-perceived QoS for data application in wireless networks was conducted. They showed that user-perceived QoS usually increases with the allocated transmission bit rate, but the increase grows slower as the rate rises beyond a certain value. Based on it, the following function is adopted to approximate the user perceived QoS [42]:

$$f(x) = 1 - e^{-x/R_s} \tag{14}$$

where x is the actual bit rate received and R_S is the maximum bit rate of the highest QoS service level of the service. The function describes the relative satisfaction from the marginal use of the service. It follows the "Law of Diminishing Marginal Utility". Namely, the marginal utility to a user’s satisfaction of receiving the bit rate from 0 kbps to 64kbps is much greater than that of receiving the bit rate from 128kbps to 192kbps. In this case, the total utility will increase fast initially then grows slower as the quantity of service consumed increases.

It has been shown that real-life economic activities such as communication service rates are all under the law of diminishing marginal utility. The price compensation of sacrificed quality is a kind of utility in economics[43]. Accordingly, we define the service charge utility function as follows:

$$g(y) = 1 - e^{\frac{-(1-y/A_{j,\max})}{1-A_{j,\min}/A_{j,\max}}} \tag{15}$$

where y is the service charge paid for the service, and $A_{j,max}$ and $A_{j,min}$ are the maximum and minimum service rates specified for the service for network type j on which the service is carried, respectively. *(1-y/$A_{j,max}$)* represents the actual charge reimbursement of the sacrificed service bit rate. We define the user satisfaction function as

$$S(x,y) = f(x) + g(y) \tag{16}$$

4.4.3. Scheduling with WF^{2}Q-M

Under the proposed service model, it is important that the service quality level specified in each service option submitted to the users once being chosen, the availability of the corresponding resources necessary is guaranteed. To meet the goal, we use the WF^{2}Q-M scheduling algorithm - a weighted fair service discipline which provides both the upper and lower bounds of transmission rate guarantees [44] to assure the transmission bit rate range of all H.264 service levels are enforced.

A WF^{2}Q-M scheduler is devised at the MAC layer in each WiMAX BS and HSDPA NodeB for outgoing packet channel access scheduling. Packets of all downstream video streaming sessions are transmitted under the WF^{2}Q-M scheduler's control to assure each session is guaranteed with a minimum service rate and subject to a maximum rate constraint according to the bit rate range of the service level of each session. In the scheduler, weight ϕ_i is allocated to session *i* of service level *l* in network type *k* as follows:

$$\phi_i^k = \frac{r_{\min}^l}{C^k} \tag{17}$$

Here, C^k is the link capacity of network type *k*. If some other sessions do not require service, the surplus capacity is redistributed among the other backlogged sessions in proportion to their respective weights subject to the maximum rate constraint.

Therefore, the actual amount of service received by a session is guaranteed to receive more than the minimum guaranteed amount but no more than the amount specified in r^l_{max}.

4.5. Performance Evaluation

In this section, we compare the number of users that can be accommodated to the cooperative network, the network resource utilization, user satisfaction and service revenue under the proposed user-decided service model with those in network-decided service model via simulation. The parameter settings in the simulation are shown in Table 6. The quality levels and service rates used are in Table 3 and 5. Three types of users are considered here: μ_{high}, μ_{medium} and μ_{low}. Each type of users has different preferences for service quality and service rate. We assume μ_{high}, μ_{medium} and μ_{low} users only accept level numbers 2 and 1.3, 1.1 and 1.2, and 1 and 1b, respectively. In the experiments, each user type randomly selects one quality level in the service request.

Table 6: The network parameters setting in simulations

	WiMAX	**HSDPA**
System Configuration	Frame per second:100	SF of DCH:128
	Slot per frame: 40	SF of HS-DSCH:16
Capacity	20 Mbps	14.4 Mbps

The arrival of user request is modeled as a Poisson process with average arrival rate λ=0.2 with equal probability of each type of users. In the network-decided service model, the first-fit policy is used – users specify no personal preference of the quality level in the service request. The service provider network checks the quality level starting from the highest level and finds the first best quality level available according to the resource state in the WiMAX/HSDPA network, and assigns it to the request. If there is a tie of available service level, the WiMAX network is chosen because it offers lower service rate.

4.5.1. Number of Users

Table 7: Number of users admitted and network utilization

	Number of Users Admitted			**Resource Utilization**		
	WiMAX	HSDPA	Total	WiMAX	HSDPA	Total
User-decided	33	16	49	85%	85%	85%
Network-decided	8	8	16	80%	71%	76%

Table 8 : The service level distribution in user-decided and network-decided model

Level number	**User-decided**		**Network-decided**	
	WiMAX	HSDPA	WiMAX	HSDPA
2	15%	14%	100%	63%
1.3	16%	16%	0%	0%
1.2	17%	17%	0%	0%
1.1	18%	18%	0%	0%
1b	17%	18%	0%	0%
1	17%	17%	0%	37%

In TABLE 7, we compare the number of users that are admitted to the network under the user-decided service model with that in the network-decided service model. One can see that under the user-decided service model, the network can accommodate three times the number of users than that using the network-decided service model. From TABLE 8, it is clear view to show the service level distribution in these two service model. The different service level achieve to uniform distribute in user-decided model, compare to network-decided the service level densely locate in high service level. This is because under the user-decided service model, the network has the flexibility to accommodate more varieties of users with different preferences for service quality and service charge. In addition, the network under the user-decided service model achieves higher resource utilization ratio.

4.5.2. User Satisfaction

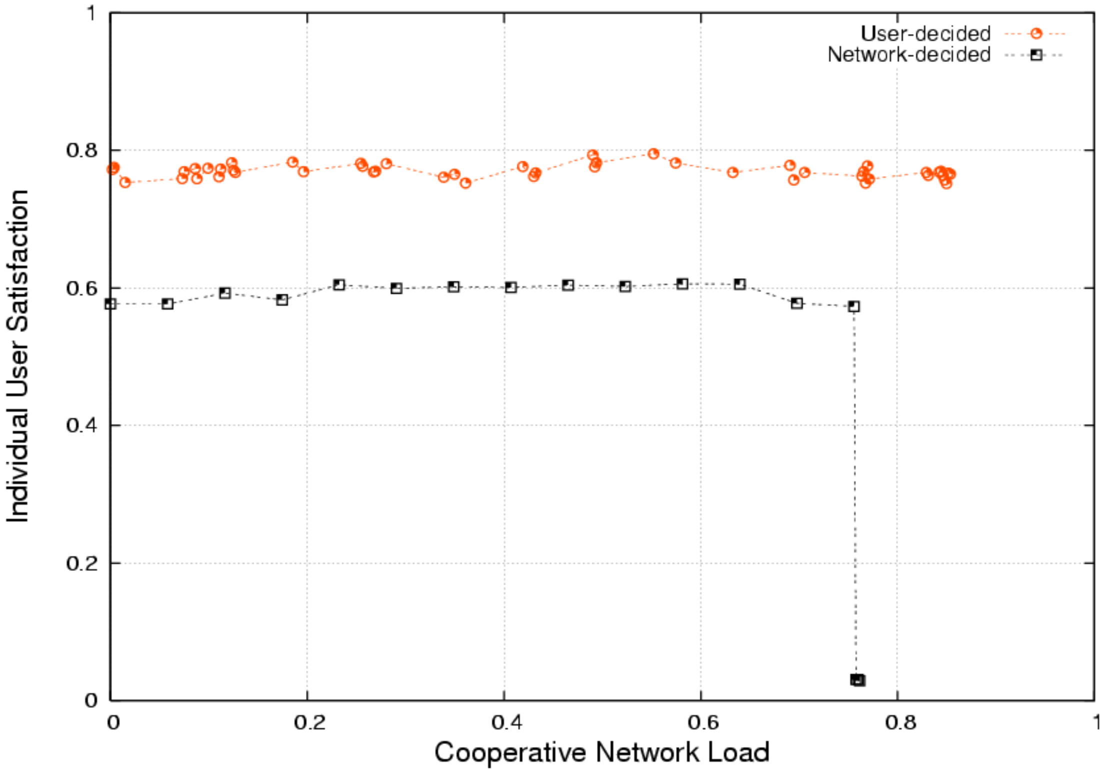


Figure 16: User satisfaction

In Fig. 16, we compare the user satisfaction of each user admitted according to equation (16) for the user-decided and network-decided service models. First, one can see that all the users admitted under the user-decided service model have higher degree of user satisfaction than those under the network-decided model. Meanwhile, the user-decided service model is able to admit more number of users.

4.5.3. Service Revenue

TABLE 9 shows the revenues received by the service provider network using the user-decided and network-decided service models. The revenue of the user-decided service model is about twice of that of the network-decided service model. This is mainly due to that the user-decided service model can accommodate more number of users to the cooperative network.

Table 9: Service revenue for network service provider

	Service Revenue		
	WiMAX	HSDPA	Total
User-decided	1760	1030	2790
Network-decided	640	800	1440

4.6. Summary of This Work

In this work, we propose a novel user-decided service model for a cooperative heterogeneous network environment. Under the model, the service provider network evaluates the state of the network and computes all possible service options. The information is then provided to the users so that they can make the final service selection according to their preferences for service quality and service charges. The rationale behind the model is that a) service provider network has complete knowledge of the network state in each network; and b) the importance of the concept of user-oriented service provisioning. We take the H.264 video streaming service and the WiMAX/HSDPA network to demonstrate how the service provider network can evaluate the feasibility of service options to support the model, as well as how to link the application’s quality level requirement to the low-layer resource management.

The simulation results show that, under the proposed model, the service network can accommodate more users, generate higher user satisfaction, and achieve higher resource utilization and revenues, compared to the network-decided service model.

The user-decided service model enables network operators to provide more flexible and efficient service to users and improve resource utilization in a cooperative network. It effectively adapts user service requests by letting users make the choices based on the possible feasible service options provided by the network to the real-time condition of the environment. This demonstrates the importance of defining the concept of user-decided service model in a cooperative heterogeneous networking environment.

5. Vertical Handoff in WiMAX/HSDPA Interworking Network

Nowadays, the wireless communications have focused on user centricity and personalization. Multiple networks have been overlaid to provide supplemented connectivity to a user. Competitve options in the current communication technologies need to be carefully studied for designing an interworking solution. A lot of works are done on interworking of UMSS(Universal Mobile Telecommunications System) with Wi-Fi. With more recent technologies like WiMAX in the market; which offers wireless broandand access with mobility support (IEEE 802.16e), and can be deployed for a wider coverage; we can interwork it with UMSS for enhancing its performance. In this Chapter, we propose a interworking architecture of WiMAX with HSDPA. In the WiMAX/HSDPA interworking model we design a component named VHOM(vertical handoff manager) which locate between these two networks, The goal of VHOM is to design an operation model to enable QoS guaranteed and seamless switchover service from one network to another in heterogeneous wireless network.

5.1. Problem Definition

Based on the proposed user-decided service model, users are given the options of choosing service level he/she is willing to pay and take. The service level is described in terms of application service quality requirements and service price. Because of vertical handoff is one of the important roaming scenarios under such a service model. It is necessary to investigate the technical feasibility of performing service level QoS guaranteed vertical handoff between heterogeneous networks. The goal of this work describes how to design an operation model to enable effective and seamless switching from one network to another. As following heterogenous network in the Chapter 4, we take the HSDPA and WiMAX as example in this work. There are three significant issues we consider in vertical handoff between heterogenous networks, separately is total handoff latency, connection packet loss, and QoS support (service level guarantee). As our knowledge, we are the first one to consider all these three issues in vertical handoff scenario.

In order to achieve seamless and QoS guaranteed vertical handoff between WiMAX and HSDPA, we propose an interworking architecture, which prove technically feasible solution for these two networks.

5.2. WiMAX/HSDPA Interworking Architecture

We based on 3GPP[5] loosely coupled approach to derive the WiMAX/HSDPA interworking architecture as shown in Fig. 17. The reasons why do we take loosely coupled approach? We have the followint two considerations which are scalability and complexity. In scalability consideration, the HSDPA and WiMAX have similar network capacity, the traffic will be aggregated in one of individual networks in tightly coupled approach, For example, if all traffics are through HSDPA core network, this will affect the original traffic planning of HSDPA. We take the advantage of traffic load sharing of loosely coupled approach in our work. The traffic will be routed through the original core network; this approach can keep the important scalability issue of two heterogeneous networks interworking together. Secondly in complexity consideration, the new entities (RNC emulator and SGSN emulator) required by WiMAX/HSDPA interworking result in a considerable increase in implementation complexity. The loosely coupled approach is much simpler and feasible compare to tightly coupled approach. In this loosely coupled scenario, no additional component is needed to be modified, i.e., we don’t need to modify the current technology and deployment. The only drawback of loosely coupled architecture is long latency, this is because handoff will cross different routing domain, care-off address is provided by FA of target network and routing information should be updated in HA.

In order to deal with the long handoff latency issue, we design a VHOM(vertical handoff manager) to avoid latency, the details are given in next section.

Based on the above disscuation, we assume WiMAX and HSDPA belong to two different operators, each operator own its AAA system and the mobile user belong to either one can switch over to another networks. The home network is responsible for access control and own its HA to handle the mobile IP process. Charging record can be generated in the visited and/or the home 3GPP network. Some assumptions in this work are listed below.

(1). A user has a dual mode device. In other words, a device has two radio access interfaces.

(2). These two networks (WiMAX and HSDPA) have a roaming agreement, we called cooperative networks as describe in Chapter 4.

(3) Two networks are peer networks and operate individually. That is to say, there is a individual HSS/AAA setup in each network.

(4). There are a handoff manager which function is to provide the information of target network through current serving network, to help UE temporally simultaneous enable two network inferfaces, this will perform soft handoff, so the services, transactions and IP connections will not break during the handoff between these two networks.

(5) Because we take loosely-coupled approach, the individual network traffic to/from a network will handle by the network itself without involving the other networks.

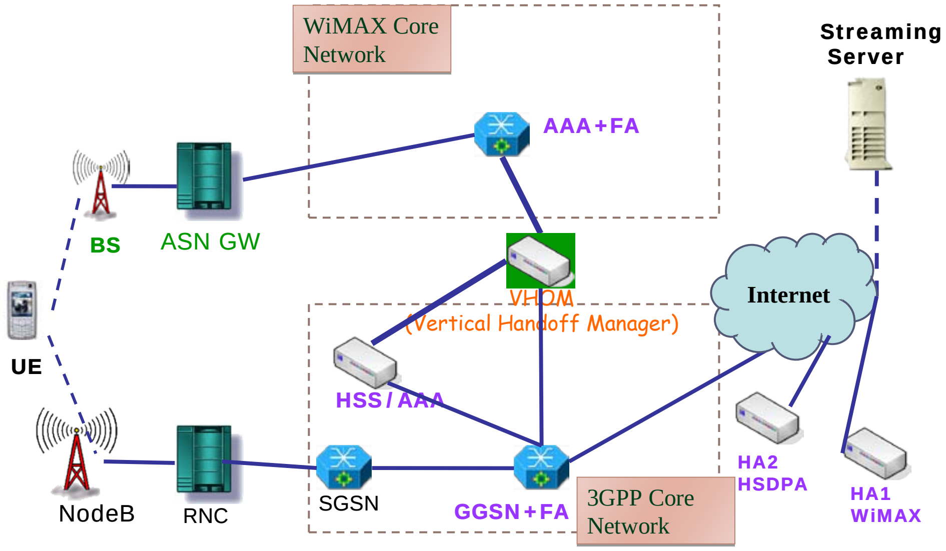


Figure 17: WiMAX/HSDPA interworking architecture

5.3. Vertical Handoff Manager

For fulfilling the seamless vertical handoff requirement, the component named Vertical Handoff Manager (VHOM) is created and located between these two networks, ref. Fig. 17. Because of these two networks are assumes to construct and operate independently, but wish to offer roaming services to their customer. The VHOM is designed for this purpose as the cooperative meant. The VHOM relays control signals and routes data packets between these two networks.

To accelerate the VHO procedure, HOM performs the following important tasks:

Separately they are querying resource of candidate networks, choosing target network, pre-authentication (AAA) and pre-registration (MIP), provides service options to UE, target network resource allocation, inform HA to do packet buffering and Data Packet Redirection.

In this thesis, introduce two handoff directions for scenario description in Section 5.3.1 and 5.3.2.

5.3.1. From HSDPA to WiMAX

As the Fig.18, 19 decipt, we broke the whole scenario into 25 steps, the details as the folloing descritions. One thing needs to be noticed here, when UE want to attach a WiMAX network, in the regular situation, UE need to contend with other UEs to grand the transmission time slot for sending ranging request, if in this short instance there is more than one UE requesting to attach this WiMAX network. In our case, before UE switch to WiMAX network as target network, VHOM already had sent information of UE to WiMAX, the target WiMAX network can pre-allocated time slot fot rhe coming UE, so called this as fast ranging in IEEE 802.16e standard.

In step 3 and 6, VHOM get the UE request and help UE to find a qualified candidate networks. After step 6, UE select option of target network and send back to VHOM. In setp 9, VHOM help UE to do pre-authentication and pre-authorization.in target network In step 11, the target network perform resource reservation. In step 15, VHOM order HA to temporarly buffer data packet of UE till step 24. In step 19, VHOM inform UE to enable the target network interface, at this moment After MIP registration finished in step 24, In setp 26, the original network resource can be released.

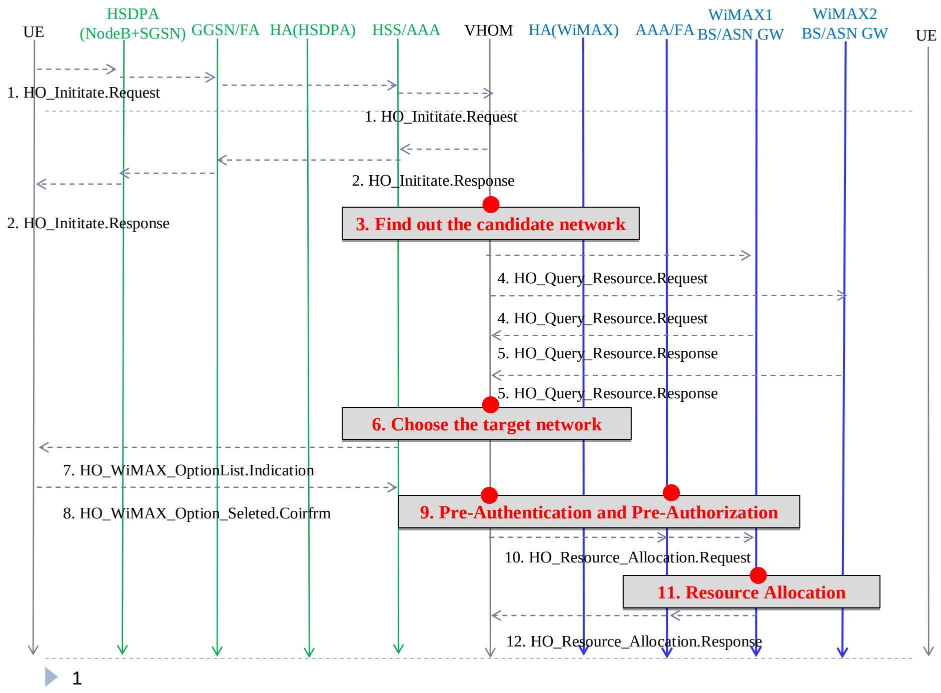

UE
HSDPA
(NodeB+SGSN)
GGSN/FA
HA(HSDPA)
HSS/AAA
VHOM
HA(WiMAX)
AAA/FA
WiMAX1
BS/ASN GW
WiMAX2
BS/ASN GW
UE
1. HO_Inititate.Request
1. HO_Inititate.Request
2. HO_Inititate.Response
2. HO_Inititate.Response
3. Find out the candidate network
4. HO_Query_Resource.Request
4. HO_Query_Resource.Request
5. HO_Query_Resource.Response
5. HO_Query_Resource.Response
6. Choose the target network
7. HO_WiMAX_OptionList.Indication
8. HO_WiMAX_Option_Seleted.Coirfrm
9. Pre-Authentication and Pre-Authorization
10. HO_Resource_Allocation.Request
11. Resource Allocation
12. HO_Resource_Allocation.Response
1

Figure 18: From HSDPA to WiMAX (1/2)

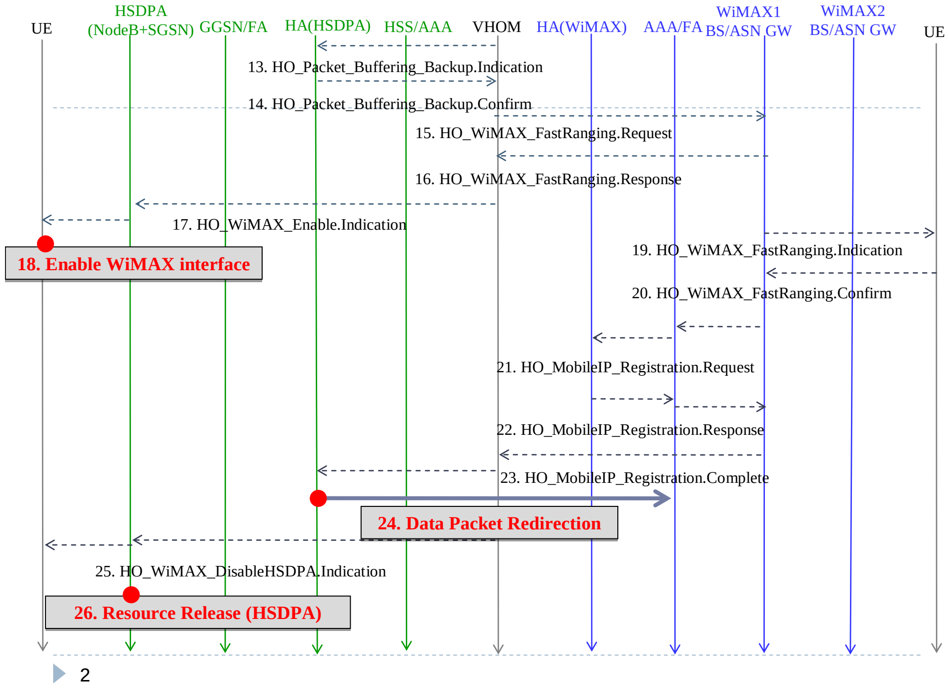
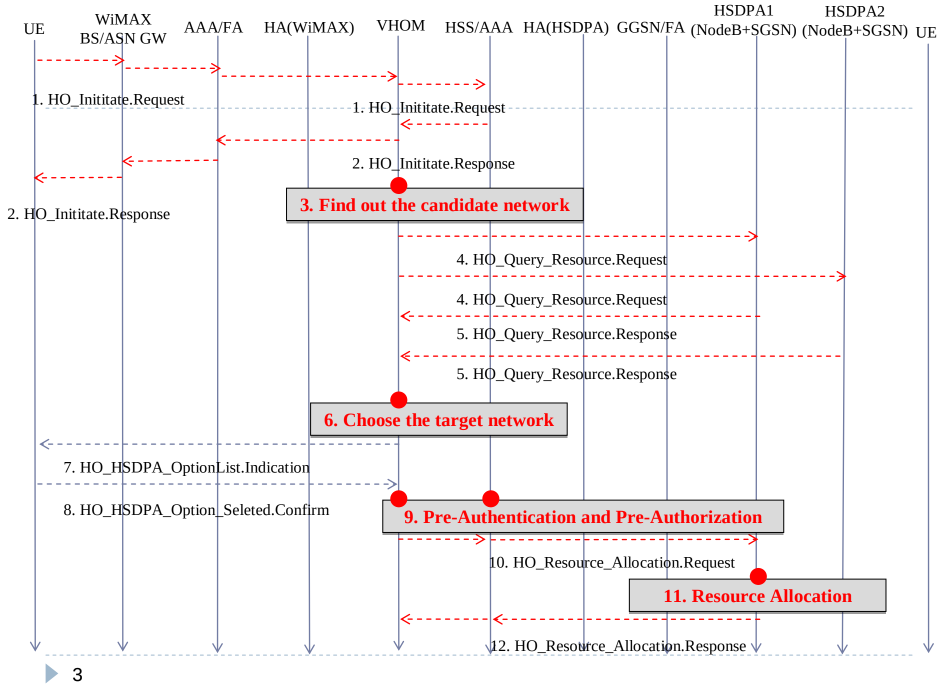

UE
HSDPA
(NodeB+SGSN)
GGSN/FA
HA(HSDPA)
HSS/AAA
VHOM
HA(WiMAX)
AAA/FA
WiMAX1
BS/ASN GW
WiMAX2
BS/ASN GW
UE
13. HO_Packet_Buffering_Backup.Indication
14. HO_Packet_Buffering_Backup.Confirm
15. HO_WiMAX_FastRanging.Request
16. HO_WiMAX_FastRanging.Response
17. HO_WiMAX_Enable.Indication
18. Enable WiMAX interface
19. HO_WiMAX_FastRanging.Indication
20. HO_WiMAX_FastRanging.Confirm
21. HO_MobileIP_Registration.Request
22. HO_MobileIP_Registration.Response
23. HO_MobileIP_Registration.Complete
24. Data Packet Redirection
25. HO_WiMAX_DisableHSDPA.Indication
26. Resource Release (HSDPA)
2

Figure 19: From HSDPA to WiMAX (2/2)

5.3.2. From WiMAX to HSDPA

Ref. Fig. 20 and 21, it is the reverse direction of section 5.3.1, similar to the same procedure as from HSDPA to WiMAX, only one different step is when perform HSDPA network entry, there is PDP(Packet Data Protocol) exchange between UE and Node B. The PDP context offers a packet data connection over which the UE and the network can exchange IP packets. Usage of these packet data connections is restricted to specific services. These services can be accessed via so-called access points.



UE
WiMAX BS/ASN GW
AAA/FA
HA(WiMAX)
VHOM
HSS/AAA
HA(HSDPA)
GGSN/FA
HSDPA1 (NodeB+SGSN)
HSDPA2 (NodeB+SGSN)
UE
1. HO_Inititate.Request
1. HO_Inititate.Request
2. HO_Inititate.Response
2. HO_Inititate.Response
3. Find out the candidate network
4. HO_Query_Resource.Request
4. HO_Query_Resource.Request
5. HO_Query_Resource.Response
5. HO_Query_Resource.Response
6. Choose the target network
7. HO_HSDPA_OptionList.Indication
8. HO_HSDPA_Option_Seleted.Confirm
9. Pre-Authentication and Pre-Authorization
10. HO_Resource_Allocation.Request
11. Resource Allocation
12. HO_Resource_Allocation.Response
3

Figure 20 : From WiMAX to HSDPA (1/2)

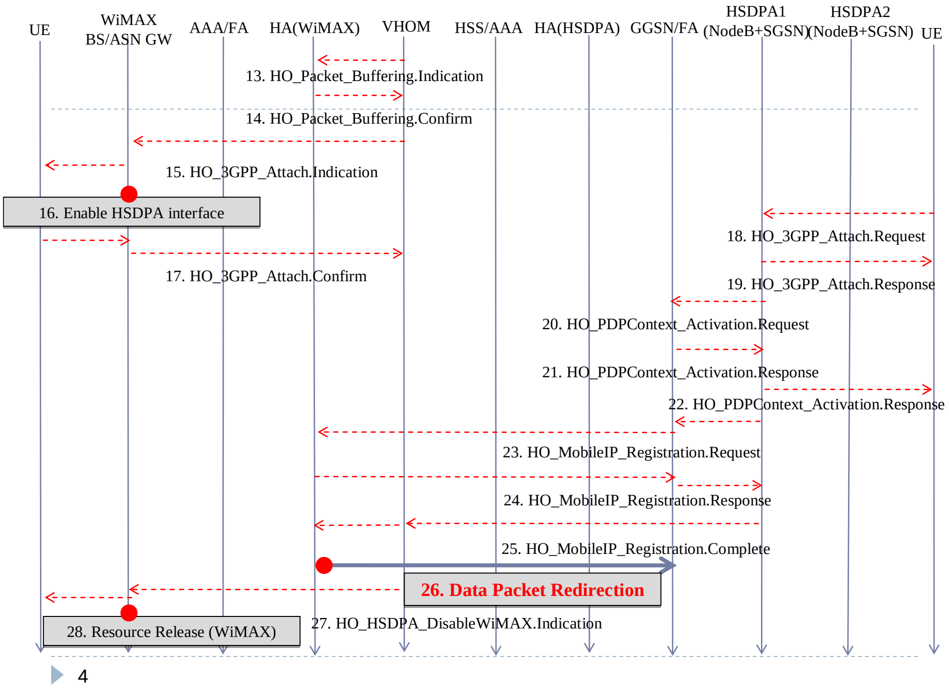

UE
WiMAX BS/ASN GW
AAA/FA
HA(WiMAX)
VHOM
HSS/AAA
HA(HSDPA)
GGSN/FA
HSDPA1 (NodeB+SGSN)
HSDPA2 (NodeB+SGSN)
UE
13. HO_Packet_Buffering.Indication
14. HO_Packet_Buffering.Confirm
15. HO_3GPP_Attach.Indication
16. Enable HSDPA interface
17. HO_3GPP_Attach.Confirm
18. HO_3GPP_Attach.Request
19. HO_3GPP_Attach.Response
20. HO_PDPContext_Activation.Request
21. HO_PDPContext_Activation.Response
22. HO_PDPContext_Activation.Response
23. HO_MobileIP_Registration.Request
24. HO_MobileIP_Registration.Response
25. HO_MobileIP_Registration.Complete
26. Data Packet Redirection
27. HO_HSDPA_DisableWiMAX.Indication
28. Resource Release (WiMAX)
4

Figure 21 : From WiMAX to HSDPA (2/2)

5.4. Performance Evaluation

In this section, we compare the service continuity probability to the cooperative heterogeneous network in handoff latency, packet loss, user satisfaction and QoS disrupt probability under the proposed VHOM assisted vertical handoff in user-decided service model with those in network-decided service of MIP based vertical handoff model via simulation. The parameters settings in the simulation are the same as section 4.5 and shown in Table 6. The quality levels and service rates used are in Table 3 and 5. In our simulation environment, there are two HSDPA radio access networks and two WiMAX radio access networks, as depicted in the Fig. 20. There are two handoff directions, the first is the UE switches from HSDPA to WiMAX, for example, UE moves from A to B, and there are two candidate WiMAX networks (WiMAX1 and WiMAX2) can be chosen. The second is UE switches from WiMAX to HSDPA, for example, UE moves from C to D, and there are two candidate HSDPA networks (HSDPA1 and HSDPA2). We assume that the UEs' QoS level in original networks is uniform distribution (level 1, 1b, …, 2). We continually increase VHO request till system saturation to calculate the QoS continuity probability in both network-decided MIP handoff and our proposed user-decided with VHOM approach.

In MIP handoff, the vertical handoff can be broken into 4 steps, shown in equation (18):

$$T_{\text{handoff,total}} = T_{\text{scan}} + T_{\text{entry}} + T_{\text{MIP}} + T_{\text{AAA}} \tag{18}$$

T_{scan} is the latency of UE to find new wireless network, if UE handoff to new wireless network, UE will first scans the correspoding frequencies of network to search candidate network, for example, in WiMAX network first to looking for downlink frequency to get DL-MAP, UL-MAP, DCD(Downlink Channel Description), UCD(Uplink Channel Description) in searching the candidate network, so called network scanning latency. T_{entry} is the latency of UE negotiate connecting paraMSers, for example, in WiMAX entry process, there is a ranging procedure to negotiate modulaton mode, power-level adjustment…etc. T_{AAA} is the latency of AAA procdure as we discussed in Chapter 3. T_{MIP} is the latency to perform binding update to reroute data packets, we had discussed in Chapter 3, too.

In MIP scenario, UE continuely receive data from serving network based on user-decided service option, if handoff occurs UE randomly choose a candidate network as the target network. However, the target network maybe cannot support the UE's service level. In our proposed approach, the VHOM will help UE choose a target network which can support the QoS level. Hence, the service level non-disruptive probability in our VHOM assisted approach is lower than than MIP based handoff in both two handoff direction, shown in Fig. 21,22.

Consider latency issues, in the VHOM assistance approch, which performs the soft handoff due to UE simultaneously, enable two wireless interfaces and excute pre-registration and pre-authenticaion in advance. Therefore, VHOM reduece the overall $T_{\text{handofftotal}}$ in equation (18), also no packet loss because VHOM order HA to buffer data packet after UE finished the vertical handoff procedure.

In VHOM solution, the service level non-disruptive point occurs till system load near 0.75 in the case from HSDPA to WiMAX.We observ that it will occur earlier service discontinuity point at system load 0.6, even at 0.4 in case WiMAX to HSDPA. This is because the HSDPA network resource is determined by SF(spreading factor) code, the allocation granularity is more rough than WiMAX.

As we discussed in user-decided service model, the user satisfaction depends on the parameters of service level option including service charge and service bit rate.

In this scenario, because the target network will be different from the original network, the service charge of corresponding level will also be different. From user's view, there is not enough information for user to choose network, therefore the VHOM should help users to choose a level of target network based on users' preference. Hence, as the same design scenario, VHOM provide the all possible options(service charge, QoS level) for user to make decision of target network.

When UE initiate service in a overlap heterogeneous wireless network area, these options will be provided to UE. In this simulation, we compare the user satisfaction in service initiation (first time enter the overlap heterogeneous networks) with the user satisfaction in target network to which UE handoff. We have two cases for two handoff directions. In case 1, users enter a HSDPA network (original network), and then they switch to a WiMAX network (new network). In case 2, users enter a WiMAX network (original network), and then they switch to a HSDPA network (new network).

The results of user-satisfaction index simulation had shown in Fig.23, one can see that all the users admitted under the user-decided service model have higher degree of average user satisfaction than those under the network-decided model. Meanwhile, after VHOM assisted vertical handoff, the average user satisfaction is still higher than under the network-decided model. We also see that after switching to WiMAX, the average user satisfaction higher than switching to HSDPA. This is because the price of WiMAX network is cheaper than HSDPA network in the same service level.

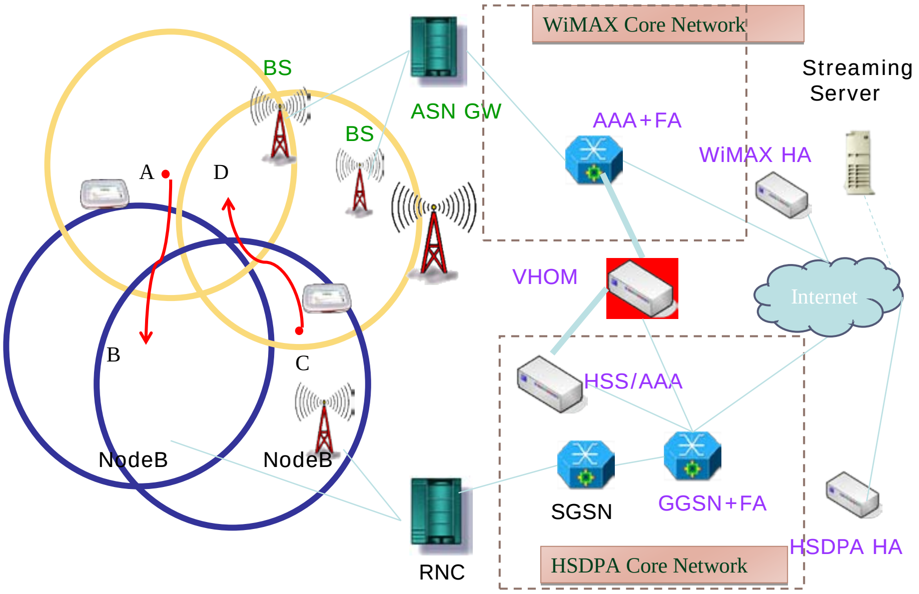


Figure 22: VHOM assisted vertical handoff network topology

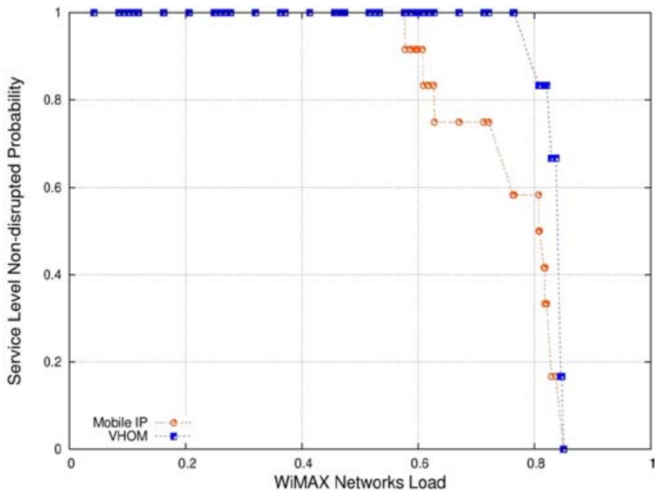


Figure 23: Service non-disruptive probability in HSDPA to WiMAX

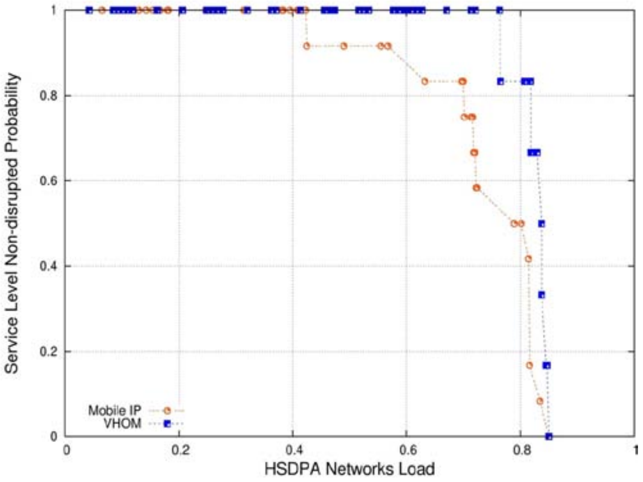


Figure 24: Service non-disruptive probability in WiMAX to HSDPA

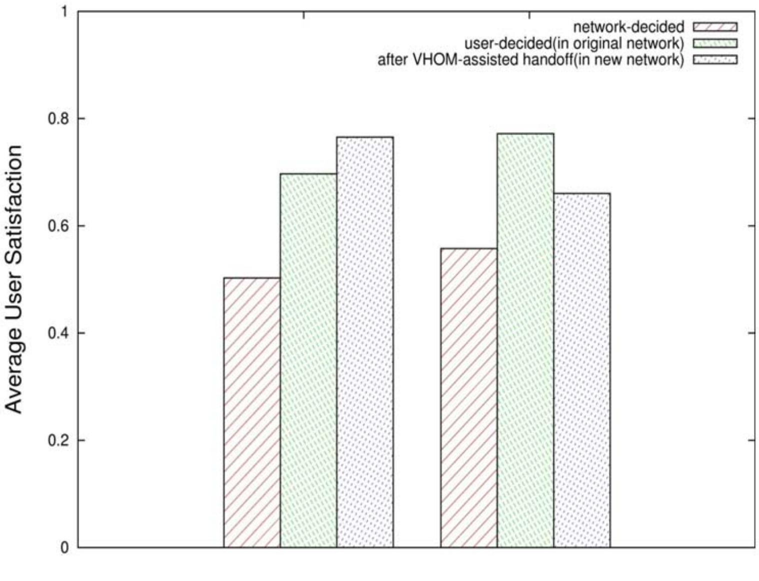


Figure 25: User satisfaction index after vertical handoff

5.5. Summary of This Work

In this work, we base on user-decided service model in a cooperative heterogeneous network environment to provide vertical handoff service. Under our vertical handoff model, UE can do vertical handoff among these overlay networks with seamless and specific user-decided service level guaranteed. We proposed a VHOM server located within these overlay networks to help handoff procedure. Before vertical handoff, UE send handoff request to VHOM server via serving network. Then VHOM evaluates the state of the networks and computes all possible service options, and send these options back for user selection. The information is then provided to the users so that they can make the final service selection according to their preferences for service quality and service charges in vertical handoff scenairo. The rationale behind the model is that a) VHOM has complete knowledge of the network state in each network; b) we take the advantage of the importance of the concept of user-oriented service provisioning. Following Chapter4, we take the H.264 video streaming service and the WiMAX/HSDPA interworking network to demonstrate in user-decided model characteristic and c) we successfully reduce vertical handoff latency and avoid packet loss, the most important is we keep the service continuity. The simulation results show that, under the proposed interworking model, the service network can generate higher user satisfaction after vertical handoff, and achieve higher resource utilization and revenues, compared to the network-decided MIP-SHO service model.

6. Conclusions and Future Work

Handoff, especially vertical handoff in wireless overlay networks has been a topic of research for over a decade now, and it is deployed in commercial products and field tests. Yet, the popularity of seamless services has not taken its place in the every day life of consumers in the same way that talking to a mobile phone or using Internet from a home PC. While there is some doubt if vertical handoff will ever have significant enough revenue creating ability for operators, the future challenge is to "put into action" services and applications that utilize vertical roaming with both technical and economical excellence. These services need to be enabled and introduced in mobile handsets with viable and tailored applications in order to see their full benefits. The challenge is about enabling better mobile applications through holistic plug-and-play connectivity and "always best connected" paradigms.

This thesis presents a holistic approach for system architecture design for the seamless and service continuity of interworking WiMAX and HSDPA networks. In the beginning of the thesis, we introduce an AAA topic when roaming occurs. In this work, we introduced there are two issues need to be taken care.   First, AAA issues are not only to deal with single sign-on to pass user authentication. Second, we need to shorten the authentication process time. In this AAA work, we address these two important issues and then propose the architecture and the protocols to form an AAA-enabled roaming alliance to allow different service operators to cooperate with one another to expedite AAA authentication/authorization to ensure non-interrupt service to mobile users. The design of U-Mobile Token successfully achieves the authentication of the issuing party and the holder as well as the integrity of U-Mobile Token by AAA servers (AAAF and AAAH), and the authentication of AAA server as a legitimate service authority by mobile node. The schemes support undeniable and of no repudiation service data records for service charging and billing. This is necessary and important between mutually un-trusted mobile user, foreign AAA and token issuer (home domain and alliance master domain) in mobile-commerce. Moreover, the U-Mobile Token is so designed to facilitate two-stage security check for not only rapid service provision to mobile user with minimal handoff latency, also with strong, rigorous service authentication and authorization.

Our design of the fast and secure universal roaming capability to mobile users which we believe is an essential feature both to provide users good service usage experience and to make the service successfully. This is fundamental and key to the success of mobile business and mobile commerce. Furthermore, base on the U-Mobile Token design, we implement FAS-URS(Fas(t) Earth) system to demonstrate the efficiency of roaming within different WISP. People can get good experience in wireless service.

Before we jump into vertical handoff, if we want user have good experience in vertical handoff service, we first need to concern what is the user wanted of wireless service? Bit rate or lower service charge? Therefore, we propose a novel user-decided service model for a cooperative heterogeneous network environment. We choose the popular wireless technologies WiMAX and HSDPA as the managed network. Under the model, the service providers should cooperate to evaluate the state of the network and computes all possible service options. The information is then provided to the users so that they can make the final service selection according to their preferences for service quality and service charges. The rationale behind the model is that a) service provider network has complete knowledge of the network state in each network; and b) the importance of the concept of user-oriented service provisioning. We take the H.264 video streaming service and the WiMAX/HSDPA network to demonstrate how the service provider network can evaluate the feasibility of service options to support the model, as well as how to link the application's quality level requirement to the low-layer resource management.

The simulation results show that, under the proposed model, the service network can accommodate more users, generate higher user satisfaction, and achieve higher resource utilization and revenues, compared to the network-decided service model.

The user-decided service model enables network operators to provide more flexible and efficient service to users and improve resource utilization in a cooperative network. It effectively adapts user service requests by letting users make the choices based on the possible feasible service options provided by the network to the real-time condition of the environment. This demonstrates the importance of defining the concept of user-decided service model in a cooperative heterogeneous networking environment

It is seen that holistic vertical system architecture design requires considerations on not only providing the basic infrastructure but also optimized functionality through a cooperative resource management to fulfill user-decied paradigm in handoff decisions. For vertical handoff, the thesis introduces a feasible technical solution in interworking architecture of WiMAX and HSDPA. Here following the user-decided service mode work, for the analysis of vertical handoff performance impact to various vertical handoff metrics including service continuity , handoff delay, packet loss, user satisfaction. In the vertical handoff topic, a VHOM server located within these overlay networks to help handoff procedure to achieve seamless and QoS guaranteed goal is designed here. Before vertical handoff, UE send handoff request to VHOM server via serving network. Then VHOM evaluates the states of the networks and computes all possible service options, and send these options back for user selection. The information is then provided to the users so that they can make the final service selection according to their preferences for service quality and service charges in vertical handoff scenairo. The rationale behind the interworking design is that a) VHOM has complete knowledge of the network state in each network; b) we take the advantage of the importance of the concept of user-oriented service provisioning. Simulation results showed that the user satisfaction increased in the VHOM assisted interworking model. Future work includes further considerations of holistic connectivity management that takes into consideration further aspects of the cross-layer approach, rules for mobility and session management, combined radio spectrum and network resource management and adaptive QoS control. The stage is open for new technological innovations: by learning from the lessons of the past; by taking advantage of existing knowledge and knowhow; and ultimately, creating something in real world.

References

[1] IAN F. A., Janise M., Joseph S. M. Ho., Huseyin U., Wenye W.,” Mobility Management in Next-Generation Wireless System,” Proc. IEEE, Vol. 87, Aug. 1999.

[2] C. Perkins, “IP Mobility Support,” RFC 2002, 1996.

[3] Campbell AT. Gomez J, Sanghvo Kim, Chieh-Yih Wan, Turanyi ZR and Valko AG, “Comparison of IP micromobility protocols,” IEEE Wireless Communications 1: 72-82, 2002.

[4] R. Ramjee, K. Varadhan, L. Salgarelli, S. Thuel, S. Wang, and T. L.Porta, “HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks,” IEEE/ACM Trans. on Networking, 2002.

[5] 3GPP TS23.234 version 7.7.0 Release 7: “Universal Mobile Telecommunications System (UMSS); 3GPP system to Wireless Local Area Network (WLAN) interworking; System description,” Technical Specification, 2008-06.

[6] IEEE 802.21/D14 Draft Standard, “Media Indepent Handover Service,” Sep. 2008.

[7] IEEE Std 802.11i/D4.1, “Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements,” July 2003.

[8] http://www.ipass.com.

[9] Valko, A. Campbell, and J. Comez., “Cellular IP”. Draft-valko-cellularip-00.txt, Nov. 1998.

[10] Charles E. Perkins and Kuang-Yeh Wang. “Optimized Smooth Handoffs in Mobile IP,” Proceedings of the Fourth IEEE Symposium on Computers and Communications, July 1999.

[11] J. Vollbrecht, etc. , “AAA Authorization Framework,” RFC 2904, 2000.

[12] J Vollbrecht, etc. , “AAA Authorization Application Example,” RFC 2905, 2000.

[13] Ted Takeyoung Kwon, Mario Gerla. “An IP-level Mobility Management Based on Quasi-Registration in Wireless Technologies Convergence,” World Wireless Congress 2002.

[14] Torsten Braun, Li Ru ,Funther Stattenberger, “An AAA Architecture Extension for Providing Differentiated Services to Mobile IP Users,” ISCC 2001.

[15] Internet Key Exchange, RFC 2409, 1998.

[16] IP Encapsulated Security Payload (ESP), RFC 2406, 1998.

[17] IP Authentication Header (AH), RFC 2402, 1998.

[18] Y. Richard Yang, X. Steve Li, X. Brian Zhang and Simon S. Lam, “Reliable Group Rekeying: A Performance Analysis,” ACM SIGCOMM, pp. 27-38, 2001.

[19] Yan Sun and K.J. Ray Liu, “Scalable Hierarchical Access Control in Secure Group Communications,” IEEE INFOCOM 2004.

[20] Thomas J. Kostas, et al,” Real-Time Voice Over Packet-Switched Networks,” IEEE Network Magazine Jan/Feb 1998.

[21] B. Aboba, J. Wood.,”Authentication, Authorization and Accounting (AAA) Transport Profile.” RFC3539, 2003.

[22] W. Diffie and M.E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory 22 (1976),” 644-654.

[23] C. W. Lee, L.M. Chen, M. C. Chen and Y. S. Sun, “A Framework of Handoffs in Wireless Overlay Networks Based on Mobile IPv6,” IEEE Journal on Selected

Areas in Communications, Volume 23, No. 11, November 2005, Pages pp.2118-2128.

[24] USAGI Project, Linux IPv6 Development Project, http://www.linux-ipv6.org

[25] A. Hess and G. Shafer,"Performance Evaluation of AAA/Mobile IP authentication," Technical Report TKN-01-012, Univ. Berlin, Aug. 2001.

[26] S. K. Miller, "Facing the Challenges of Wireless Security," IEEE Computer, pp. 46–48, July 2001.

[27] W.A. Arbaugh, "Wireless security is different," IEEE Computer, pp.99-101,2 Aug. 2003.

[28] H. J. Wang, R.H. Katz, and J. Giese, "Policy-Enabled Handoffs across Heterogeneous Wireless Networks," Proc. IEEE Workshop, Mobile Computation Systems and Applications, February 1999.

[29] Mani, N. Crespi, "Handover Criteria Considerations in Future Convergent Networks," IEEE Globecom 2006.

[30] A. Hasib, A.O. Fapojuwo, "Joint Radio Resource Management over Very Tightly Coupled Heterogeneous Networks for Multimode Reconfigurable Terminals," IEEE VTC 2006.

[31] S. Horrich, S. E. Elayoubi and S. B. Jemaa, "A game-theoretic model for radio resource management in a cooperative WIMAX/HSDPA network," IEEE ICC 2008.

[32] P. Mahonen, M. Petrova, J. Riihijarvi, and M. Wllens, "Cognitive Wireless Networks: Your Network Just Became a Teenager," IEEE INFOCOM Poster 2006.

[33] "Information technology — Coding of audio-visual objects H.264/AVC", International Standard ISO/IEC 14496-10, 2004.

[34] IEEE. 802.16e-2005: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. Standard, February 28, 2006.

[35] 3GPP TS 25.213 "Spreading and modulation (FDD) (R7)," November, 2007.

[36] http://www.ntt-east.co.jp/product_e/05/2.html, NTT EAST Monthly Charge of ADSL.

[37] http://www.cht.com.tw, Chunghwa Telecom Monthly Charge of ADSL.

[38] N. P. Melone, "A Theoretical Assessment of the User-Satisfaction Construct in Information Systems Research Management Science," Management Science, Vol. 36, No. 1, pp. 76-91, January, 1990.

[39] W. R. Scott," Organizational Effectiveness," in Organizations: Rational, Natural, and Open (2nd edition), Prentice-Hall, Englewood Cliffs, NJ, 1987.

[40] L. T. Su, "The relevance of recall and precision in user evaluation," Journal of the American Society for Information Science and Technology, Volume 45, Jan, 1999, pp. 207 – 217.

[41] Z. Jiang, H. Mason., J. Kim., N. K. Shankaranarayanan and P. Henry. "A Subjective Survey of User Experience for Data Application in Future Cellular Wireless Networks," Proceedings of SAINT. 2001.

[42] N Enderlé, X. Lagrange, "User Satisfaction Models and scheduling algorithms for packet-switched services in UMSS," IEEE VTC 2003.

[43] YK Ng, "A Case for Happiness, Cardinalism, and Interpersonal Comparability," Vol. 107, NO 445, 1997, pp. 1848-1858.

[44] J. F. Lee, M. C. Chen and Y. S. Sun, "WF2Q-M: Worst-case Fair Weighted Fair Queueing with Maximum Rate Control," Computer Networks, Vol. 51, pp. 1403-1420, 2007.

[45] Mark Stemm and Randy H. Katz, “Vertical handoffs in wireless overlay networks,” Mobile Networks and Applications, ACM MONET, Summer 19.

[46] V. Varma, S. Ramesh, K.D. Wong, M. Barton, G. Hayward and J. Friedhoffer. “Mobility Management in Integrated UMSS/WLAN Networks,” IEEE ICC 2003.

[47] Hyun-Ho Choi, Song, O.; Dong-Ho Cho; ”A seamless handoff scheme for UMSS/WLAN interworking,” IEEE Globecom 2004.

Appendix: Handoff Message Description

The proposed HO message – HO_Query_Resource.Request

Message Name{data memeber}	Description

HO_Query_Resource.Request{
SourceIdentifier,
DestinationIdentifier,
GeographicLocation,
}
	Before transmitting this message, according to the location information, HOM find out the candidate networks from its database which collects the associated network in advance.
	After that, HOM sends the HO_Query_Resource.Request to each candidate network founded from the database.
	When the candidate networks receives this message, by referring to the GeoGraphicLocation field, they estimate the probable receive signal strength for UE in corresponding candidate network.

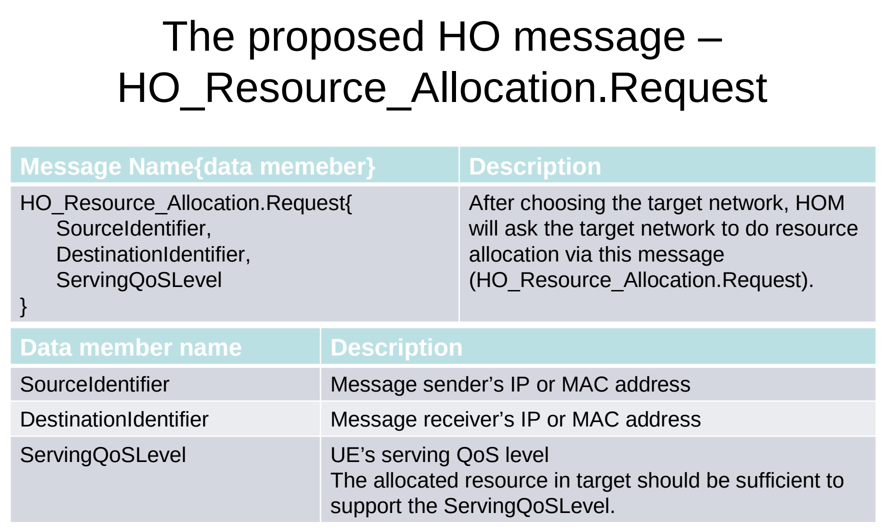
Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
GeographicLocation	UE’s geographic location information(will be provided by Location Based Service)

The proposed HO message – HO_Query_Resource.Response

Message Name{data memeber}	Description

HO_Query_Resource.Response{
SourceIdentifier,
DestinationIdentifier,
….,
AvailableQoSLevel
}
	When UE’s received signal strength is hard to support it’s current service, it will send this message to serving BS/NodeB to do information request, i.e., handoff request.
	In this message, UE provide its handoff related information which detailed in the following table.

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
EstimatedReceivedSignalStrength	The UE’s probable Received Signal Strength in the candidate network(sender of this message) When the HOM has received this message, it chooses the target network based on both EstimatedReceivedSignalStrength and AvailableQoSLevel fields.
AvailableQoSLevel	The available QoS Level supported in this candidate network(sender of this message) HOM will choose the network witch can provide the best AvaiableQoSLevel of all candidate networks as the HO target network. If there exists some candidate networks providing the same AvailbleQoSLevel, HOM will choose the one with highest EstimatedReceivedSignalStrength from them.

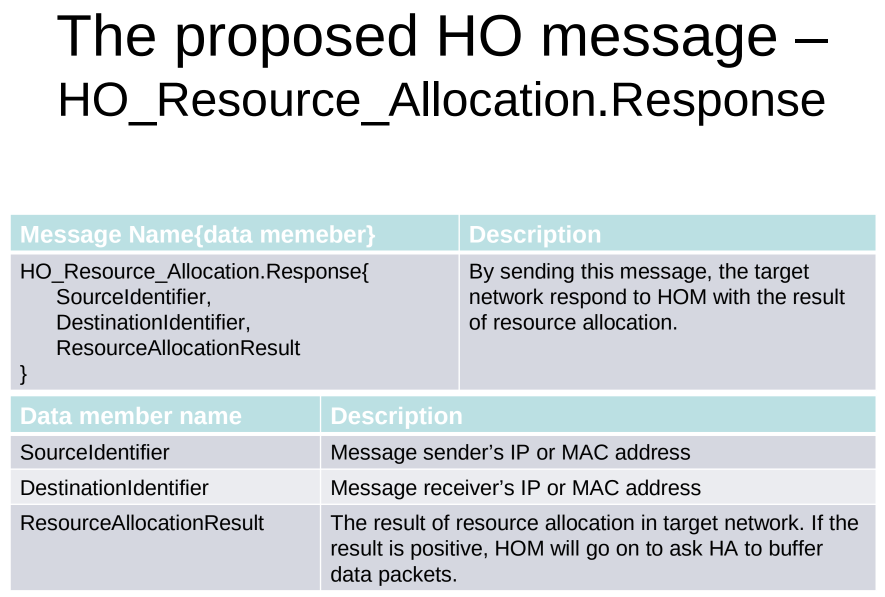


The proposed HO message – HO_Resource_Allocation.Request

Message Name{data memeber}	Description

HO_Resource_Allocation.Request{
SourceIdentifier,
DestinationIdentifier,
ServingQoSLevel
}
	After choosing the target network, HOM will ask the target network to do resource allocation via this message (HO_Resource_Allocation.Request).

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
ServingQoSLevel	UE’s serving QoS level The allocated resource in target should be sufficient to support the ServingQoSLevel.

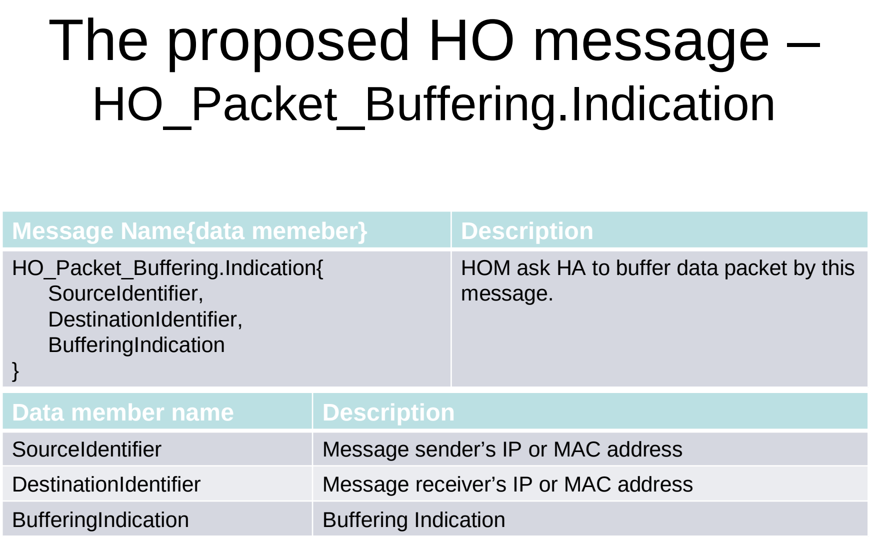


The proposed HO message – HO_Resource_Allocation.Response

Message Name{data memeber}	Description

HO_Resource_Allocation.Response{
SourceIdentifier,
DestinationIdentifier,
ResourceAllocationResult
}
	By sending this message, the target network respond to HOM with the result of resource allocation.

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
ResourceAllocationResult	The result of resource allocation in target network. If the result is positive, HOM will go on to ask HA to buffer data packets.

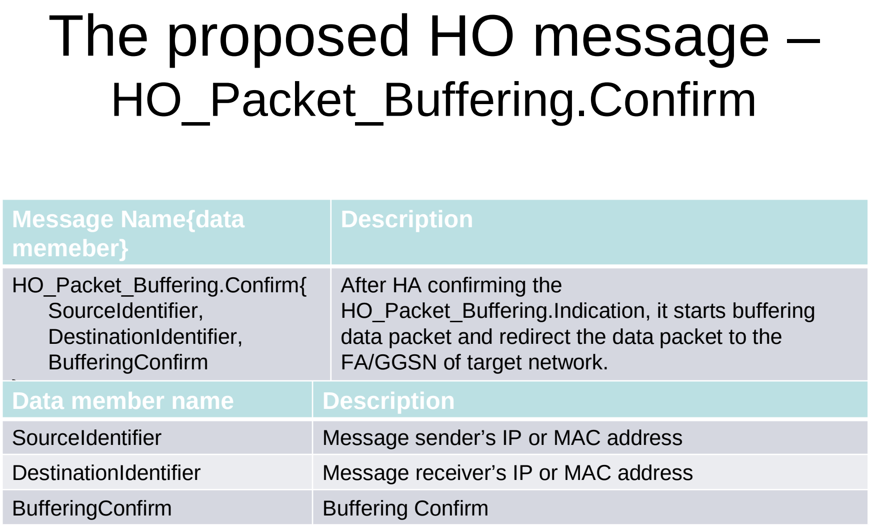


The proposed HO message – HO_Packet_Buffering.Indication

Message Name{data memeber}	Description

HO_Packet_Buffering.Indication{
SourceIdentifier,
DestinationIdentifier,
BufferingIndication
}
	HOM ask HA to buffer data packet by this message.

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
BufferingIndication	Buffering Indication



The proposed HO message – HO_Packet_Buffering.Confirm

Message Name{data memeber}	Description
HO_Packet_Buffering.Confirm{ SourceIdentifier, DestinationIdentifier, BufferingConfirm	After HA confirming the HO_Packet_Buffering.Indication, it starts buffering data packet and redirect the data packet to the FA/GGSN of target network.

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
BufferingConfirm	Buffering Confirm

The proposed HO message –
HO_3GPP_Attach.Indication

Message Name{data memeber}	Description

HO_3GPP_Attach.Indication{
SourceIdentifier,
DestinationIdentifier,
TargetNetworkNodeBID
3GPPAttachIndication
}
	Using this message, HOM notice UE to start 3GPP attachment procedure.

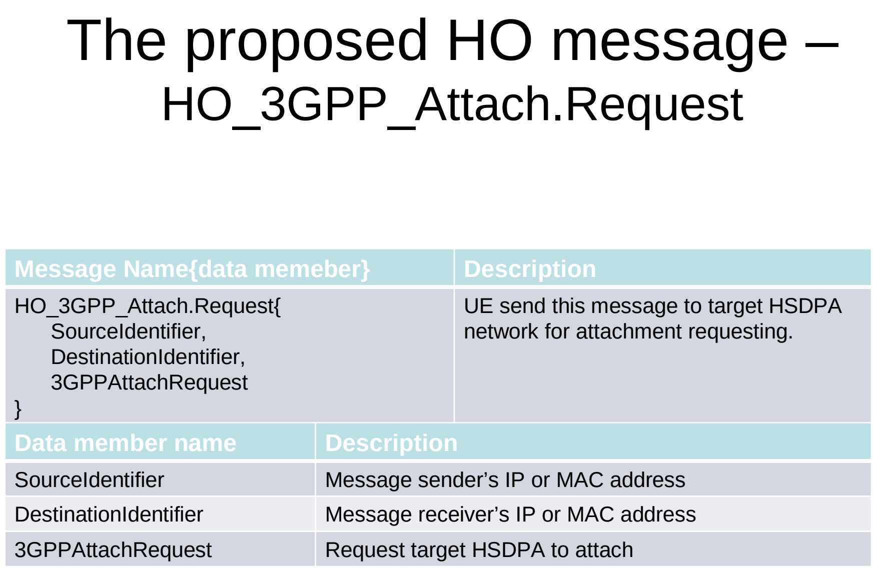
Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
TargetNetworkNodeBID	The NodeB ID of target network
3GPPAttachIndication	3GPP attachment indication

The proposed HO message –
HO_3GPP_Attach.Confirm

Message Name{data memeber}	Description

HO_3GPP_Attach.Confirm{
SourceIdentifier,
DestinationIdentifier,
3GPPAttachConfirm
}
	After this message, UE start attaching the target 3GPP network (HSDPA in our case).
	This message also indicate that WiMAX network can release its resource.

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
3GPPAttachConfirm	UE’s 3GPP attachment confirm

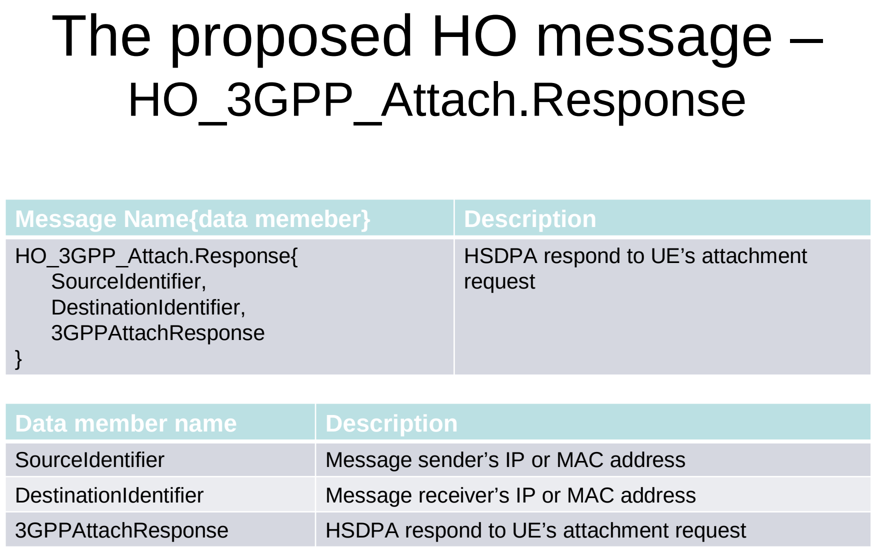


The proposed HO message – HO_3GPP_Attach.Request

Message Name{data memeber}	Description

HO_3GPP_Attach.Request{
SourceIdentifier,
DestinationIdentifier,
3GPPAttachRequest
}
	UE send this message to target HSDPA network for attachment requesting.

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
3GPPAttachRequest	Request target HSDPA to attach



The proposed HO message – HO_3GPP_Attach.Response

Message Name{data memeber}	Description

HO_3GPP_Attach.Response{
SourceIdentifier,
DestinationIdentifier,
3GPPAttachResponse
}
	HSDPA respond to UE's attachment request

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
3GPPAttachResponse	HSDPA respond to UE's attachment request

The proposed HO message – HO_PDPContext_Activation.Request

Message Name{data memeber}	Description

HO_PDPContext_Activation.Request{
SourceIdentifier,
DestinationIdentifier,
PDPContextRequest
}
	The target HSDPA send this message to its GGSN for PDP context activation.

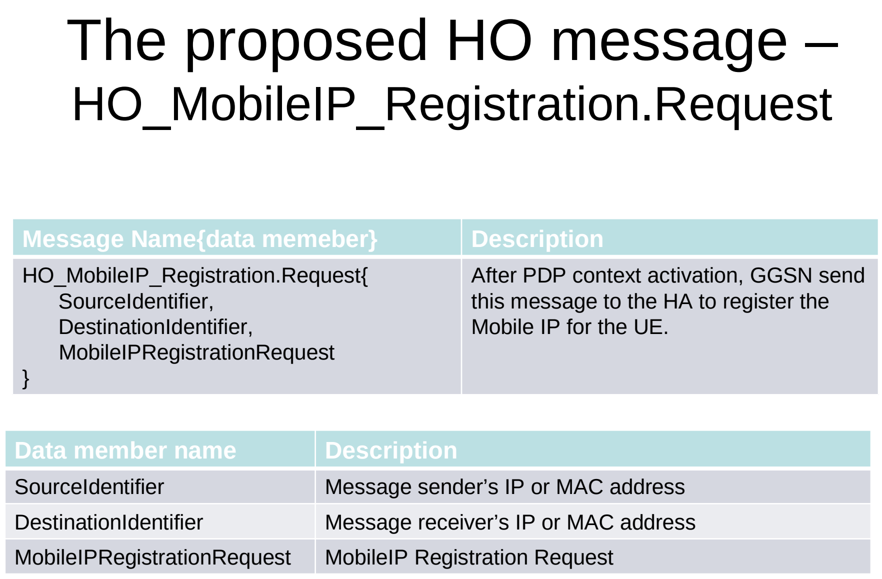
Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
PDPContextRequest	PDP Context activation request

The proposed HO message – HO_PDPContext_Activation.Response

Message Name{data memeber}	Description

HO_PDPContext_Activation.Response{
SourceIdentifier,
DestinationIdentifier,
PDPContextResponse
}
	GGSN respond to the target HSDPA and activate the PDP context.

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
PDPContextResponse	PDP Context activation response

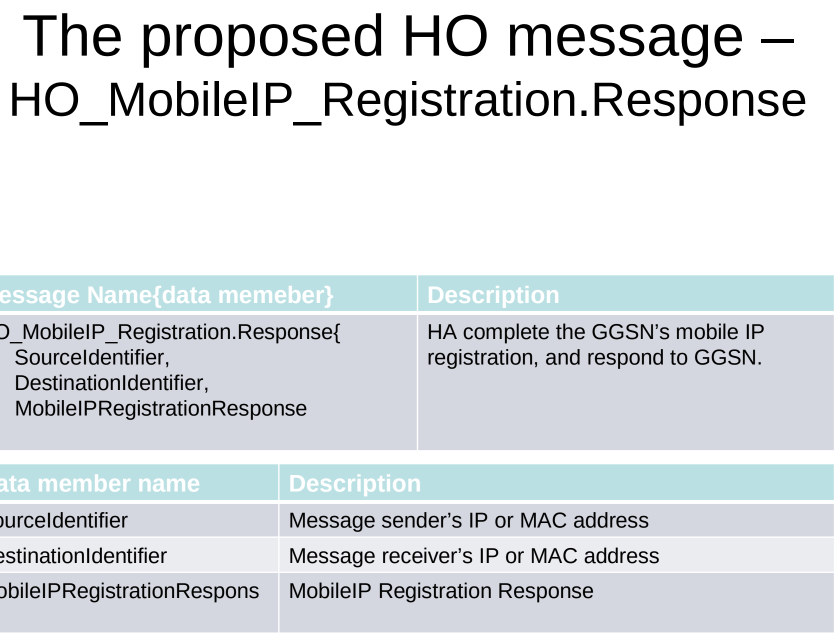


The proposed HO message – HO_MobileIP_Registration.Request

Message Name{data memeber}	Description

HO_MobileIP_Registration.Request{
SourceIdentifier,
DestinationIdentifier,
MobileIPRegistrationRequest
}
	After PDP context activation, GGSN send this message to the HA to register the Mobile IP for the UE.

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
MobileIPRegistrationRequest	MobileIP Registration Request

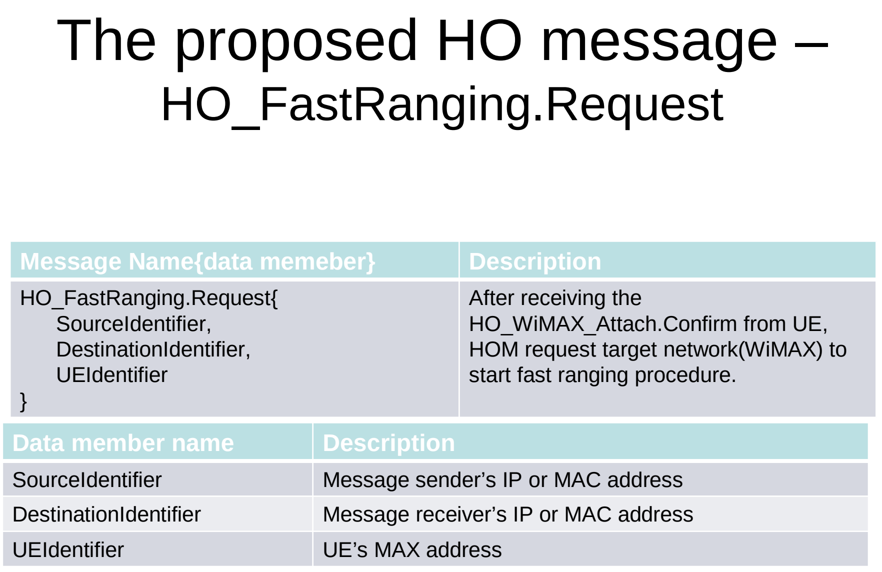


The proposed HO message – HO_MobileIP_Registration.Response

Message Name{data memeber}	Description

HO_MobileIP_Registration.Response{
SourceIdentifier,
DestinationIdentifier,
MobileIPRegistrationResponse
}
	HA complete the GGSN's mobile IP registration, and respond to GGSN.

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
MobileIPRegistrationRespons e	MobileIP Registration Response

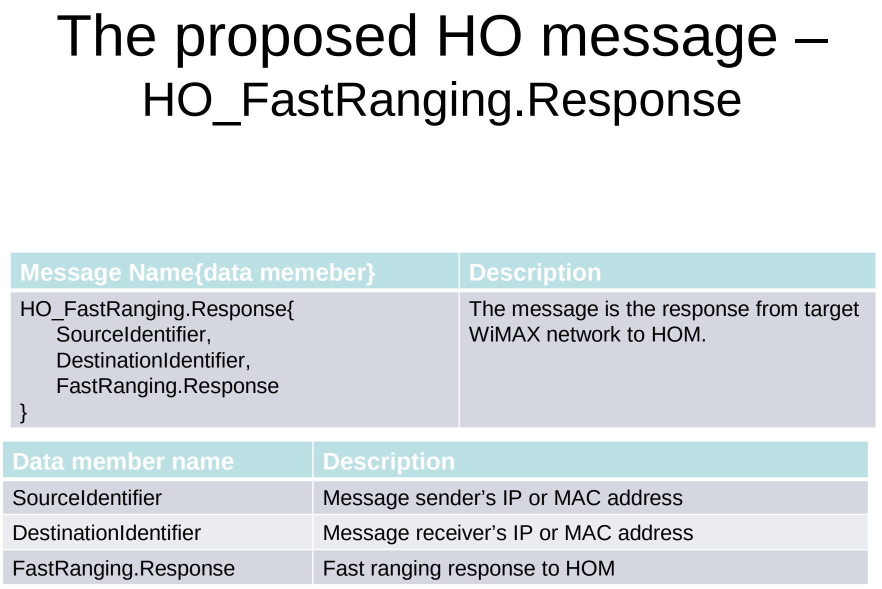


The proposed HO message – HO_FastRanging.Request

Message Name{data memeber}	Description

HO_FastRanging.Request{
SourceIdentifier,
DestinationIdentifier,
UEIdentifier
}
	After receiving the HO_WiMAX_Attach.Confirm from UE, HOM request target network(WiMAX) to start fast ranging procedure.

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
UEIdentifier	UE's MAX address

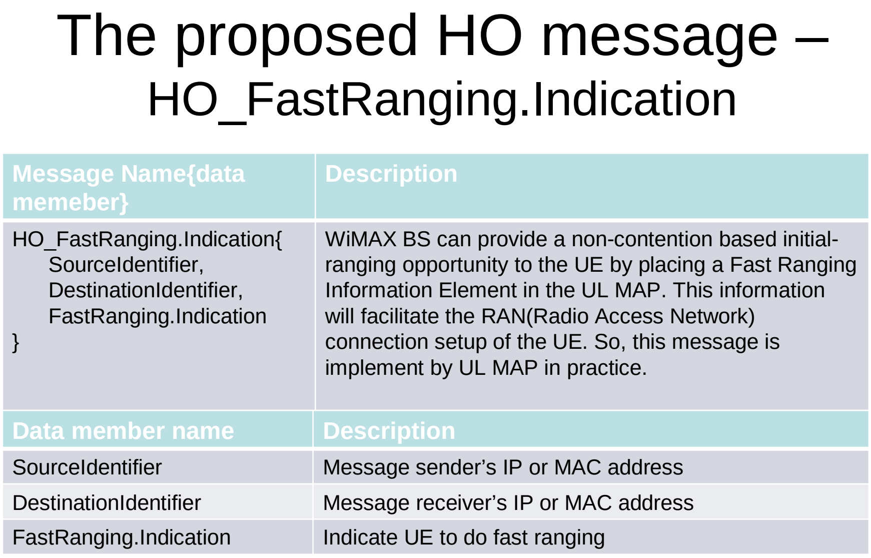


The proposed HO message – HO_FastRanging.Response

Message Name{data memeber}	Description

HO_FastRanging.Response{
SourceIdentifier,
DestinationIdentifier,
FastRanging.Response
}
	The message is the response from target WiMAX network to HOM.

Data member name	Description
SourceIdentifier	Message sender's IP or MAC address
DestinationIdentifier	Message receiver's IP or MAC address
FastRanging.Response	Fast ranging response to HOM



The proposed HO message – HO_FastRanging.Indication

Message Name{data memeber}	Description

HO_FastRanging.Indication{
SourceIdentifier,
DestinationIdentifier,
FastRanging.Indication
}
	WiMAX BS can provide a non-contention based initial-ranging opportunity to the UE by placing a Fast Ranging Information Element in the UL MAP. This information will facilitate the RAN(Radio Access Network) connection setup of the UE. So, this message is implement by UL MAP in practice.

Data member name	Description
SourceIdentifier	Message sender’s IP or MAC address
DestinationIdentifier	Message receiver’s IP or MAC address
FastRanging.Indication	Indicate UE to do fast ranging