國立交通大學

資訊學院 資訊學程

碩士論文

支援WiMAX網路快速換手之分散式金鑰配置機制

A Distributed Key Assignment Mechanism for Fast Handover in WiMAX Networks

研 究 生：陳亭翰
指導教授：曾建超 教授

中 華 民 國 九 十 六 年 七 月

支援 WiMAX 網路快速換手之分散式金鑰配置機制
A Distributed Key Assignment Mechanism for Fast Handover in WiMAX Networks

研 究 生：陳亭翰　　Student：Ting-Hang Chen
指導教授：曾建超　　Advisor：Chien-Chao Tseng

國 立 交 通 大 學

資訊學院　資訊學程

碩 士 論 文

A Thesis
Submitted to College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of

Master of Science
in

Computer Science

July 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年七月

支援 WiMAX 網路快速換手之分散式金鑰配置機制

學生：陳亭翰　　指導教授：曾建超

國立交通大學　資訊學院　資訊學程碩士班

摘　要

本論文依據 IEEE802.16e 與 WiMAX Forum 中 Network Working Group (NWG)制定的換手協定，修改換手過程時的金鑰派送與傳送機制，以減少 WiMAX 後端網路的負擔爲目標，達到快速換手的目的。

IEEE802.16e 的換手程序包含金鑰的重新派送，因此 NWG 也定義了後端(backhaul)網路產生與派送金鑰的金鑰更新機制。也就是說，每次的換手程序都必定在後端網路執行一次金鑰的產生及派送的動作。這樣的作法不僅會增加後端網路的負擔，更新金鑰的動作也會增加換手延遲。

針對此問題，本論文提出一個分散式的金鑰配置機制，在不失安全性的前提下，藉由擴大金鑰有效範圍，減少了換手過程中執行金鑰產生與派送程序的次數，藉以減少換手時所產生的後端網路資訊量。也因此，改善了換手程序所需的平均換手時間。

最後，本論文也進一步分析及探討我們提出的方法的安全性，確定此方法在運作上不失其安全性；另一方面，本論文也利用數學分析，比較此方法與 NWG 所制定的方法，證明了本論文的方法在減少網路負載上較爲優異，也因此改善了換手程序所需的平均換手時間。

A Distributed Key Assignment Mechanism for Fast Handover in WiMAX Networks

Student: Ting-Hang Chen Advisor: Chien-Chao Tseng

Degree Program of Computer Science
National Chiao Tung University

ABSTRACT

This thesis proposes a distributed key assignment mechanism that can support fast handover for WiMAX networks. According to the specifications of IEEE 802.16e and Network Working Group (NWG) of WiMAX forum, a WiMAX mobile station (MS) needs to perform a key re-assignment for each handover procedure. The key re-assignment procedudre requires several message exchanges between the MS and the authentication server situated in the backhaul network. Therefore, it not only introduces signal overhead to the backhaul network but also increases the latency of handover procedures.

The underlying concept of the distributed key assignment mechanism is to enlarge the scope of the authentication key (AK) so that the MS needs not perform an AK re-assignment each time it roams from one base station to another. By reducing the number of key re-assignments, the proposed mechanism can reduce both the number of signals in backhaul networks and the handover latency, while retaining the same security level as the original WiMAX does.

We also present an analytical model to evaluate the proposed key assignment mechanism. Analytical results show that the proposed mechanism can not only reduce signal overhead in backhaul networks but also shorten the handover latency. Furthermore, we also analyze the security level of the proposed mechanism to justify the effectiveness of the proposed mechanism.

誌　　謝

工作了六年多，一直渴望能夠再回到學校進修，如今終於能按照自己的理想目標一步一步的邁進，心中的感受自是無法言喻。而當我在完成這篇論文著作時，對於那些曾經幫助我，協助我完成著作的人，內心充滿無限感激。

這篇論文的完成，首先的得感謝指導教授：曾建超博士。在這兩年的論文研究裡，曾博士尊重我、允許我研究我所興趣的題目，並指導我研究的態度及方法，以及邏輯思考的能力。此外，還要感謝論文口試委員鄭瑞光博士、曹孝櫟博士、楊人順博士對於本論文提供寶貴的意見，讓本論文更爲嚴謹與完備。

還要感謝無線網際網路實驗室的學長：王瑞堂、黃貴笠，一路陪我從論文的構思到整篇論文的順利完成，給予我觀念上的指正，以及技術上的栽培。還要感謝同學的幫忙，有了各位一起唸書、趕作業、拚考試，才能夠順利修完這兩年的課程。

最後，還要感謝我工作上的夥伴，始終協助我並分擔我的工作項目，使我有足夠時間完成兩年學業。一路上支持我陪伴我的女友雅惠，總是體諒我，分擔我的壓力與難過。養育我的父母以及我的家人，不停地給予我精神上的鼓勵與支持。

感謝大家對我的關心，在這一篇幅中，與各位分享我完成論文的喜悅。

表目錄

圖目錄


E
S
A
1896

第 1 章
序論

1.1 研究動機

隨著無線網路的快速發展，無線網路技術由紅外線傳輸、藍芽、IEEE802.11進展到目前各界極力推廣的無線網路新主流—IEEE802.16。一方面 IEEE 組織持續制定其相關規格與改良技術，另一方面 WiMAX (Worldwide Interoperability for Microwave Access)聯盟(WiMAX Forum)依據 IEEE 所訂定的標準提供 WiMAX 網路後端(backhaul)的整合設計。

WiMAX 標準規格爲 IEEE 802.16，包含固定式的 IEEE802.16d 與提供移動的 IEEE802.16e，用以滿足市場不同的需求。WiMAX 之所以獲得青睞，在於 WiMAX 爲新的無線傳輸網路技術，有傳送距離遠、覆蓋範圍廣、傳輸量(throughput)高、支援語音與影像的服務品質 QoS (quality of service)以及安全性設計等的特性。

在 IEEE802.16e 裡，因安全性考量，當 mobile station (MS) 執行換手動作(handover)時，一定會與目標基地台(target base station)建立一新的安全性連結。這樣的行爲所帶來的影響有三：

1) 增加WiMAX後端網路(backhaul)額外的負擔。

2) 換手過程中，MS需因等待網路後端的傳送與計算所造成時間延遲。

3) 對於即時性的應用軟體來說(real-time application)，如VoIP (Voice over Internet Protocol)，因延遲而影響通話品質。

本論文針對於WiMAX的安全性考量以及QoS的效能，提出一套方法，在秉持IEEE802.16的設計精神且不影響安全性的情形下，減少換手延遲時間。

1.2 研究目標

WiMAX後端網路分爲兩個區塊(Figure 1-1WiMAX網路架構)，一爲Network Access Provider (NAP)，由一個或多個Access Service Network (ASN)所組成，其中組成元件包含有BS、Authenticator、ASN-GW (Access Service Network Gateway)，負責MS在WiMAX無線網路的存取；另一區塊爲Network Service Provider (NSP)，包含有H-AAA (Home AAA) server、GW Router等元件，負責IP層的網路連線與提供WiMAX網路服務功能。

當MS在一開始(initial network entry)爲了要能夠允許進入WiMAX網路，必須先執行認證過程。因此MS認證封包的行經路線爲經由BS、Authenticator、ASN-GW穿透到NSP與AAA server來進行認證(Figure 1-2)。在IEEE802.16e定義到MS認證的兩種方式： RSA與EAP (Extensible Authentication Protocol)。但在WiMAX Forum裡的Network Working Group (NWG)明確指出WiMAX Forum已捨棄RSA認證模式(參照[4])，只支援EAP的認證模式，因此本論文只討論EAP的認證過程。

MS在一開始申請進入網路階段，透過EAP的認證模式，MS與AAA server進行一連串EAP的標準認證過程，在AAA的許可之下，最終由Authenticator負責配送一把金鑰(AK)給BS，MS也自行產生一把AK。AK的最主要目的在於建立BS與MS之間共用一把金鑰，作爲往後資料傳輸及驗證所必須的前提。當MS換手到另外一台BS時，MS會產生一把新的AK，理所當然Authenticator也必須要建立一把新的AK給BS。因此，在WiMAX環境下，由於BS的覆蓋範圍廣大(理論上可達 30 公里到 50 公里，實際測試約爲 8 公里[9])，隨著底下的MS數量增多，對WiMAX後端網路來說，頻繁的換手(handover)過程均需要重新產生AK，所以爲產生AK而進行一連串的溝通訊息將大大的增加WiMAX後端網路的負擔。此外，Authenticator爲產生BS與MS之間共用的AK而必須進行數學運算，也加重了Authenticator的負擔。對MS來說，MS必須等待BS獲得AK後始得與BS進行AK的驗證，待驗證成功後，資料才可以進行傳輸。這對即時的應用程式(如VoIP) 來說，會嚴重影響通訊品質。

本論文著眼於此，最主要的目的，在於 AK 產生的過程中，必須兼顧安全性的考量下：

1) 減少 WiMAX 後端訊息傳送過程；
2) 減少 Authenticator 的運算負擔；
3) 達成無接縫的效果(seamless)以減少即時應用軟體因換手而出現訊號間斷或延遲的情形；
4) 降低認證與換手的相依性，使換手過程不因認證過程導致延遲。

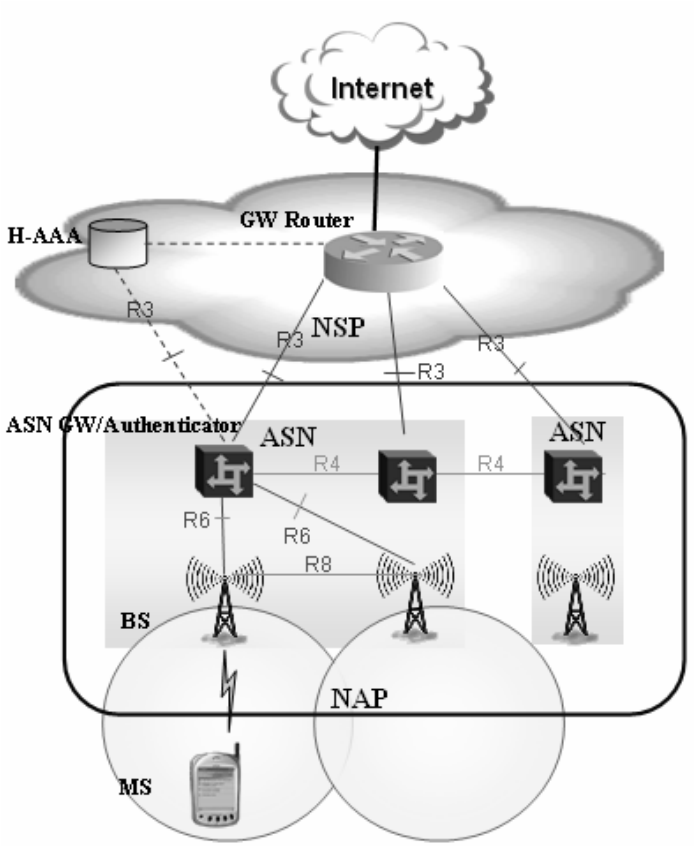


Figure 1-1WiMAX 網路架構

Figure 1-2 MS 認證的行經路線

1.3 論文內容

關於本篇論文的內容簡述如下：

第一章“序論”

描述這篇論文的研究動機，以及這篇論文希望達到的目標。

第二章“研究背景與相關論文研究”

在提出本論文的解決方案之前，先瞭解 IEEE802.16 以及 NWG 如何規劃整個 WiMAX 網路在 initial network entry 階段以及換手階段的認證與授權流程。本章節將詳細介紹整個 WiMAX 網路環境，並且在此環境下如何運作認證與授權流程。

第三章“Distributed security mechanism”

詳細描述本論文的解決方案；針對換手所造成的延遲性，透過修改 IEEE 以及 NWG 裡所制定的認證與授權流程，來改進其缺點，並對提出的方案作多項分析。

第四章“實作分析”

介紹實驗的環境模型(model)以及對本論文的解決方案列出數學分析式。根據實驗數據分析其結果印證本論文的論述。

第五章“結論與未來工作”

描述本論文當初設計的各種可行性分析以及針對論文所提的方法作出實驗結論並提出未來可繼續研究的方向。

第 2 章
研究背景與相關論文研究（Related work）

本章節首先介紹網路工作群組(NWG)如何定義前端(MS 與 BS 之間)與後端(backhaul)的網路架構以及認證架構。瞭解 WiMAX 整體環境後，則開始詳述 MS 在 initial network entry 階段時，IEEE802.16e 如何制定 MS 與 BS 之間的認證與授權程序，以及後端(backhaul)網路如何配合 IEEE 802.16 制定運作流程。接下來描述啓動換手程序時，WiMAX 系統對於有關於安全性(security)的處理方式。主要針對 AK 的如何取得與分配會加以提出說明，其中包括：啓動換手的時機點、MS 在不同區域(domain)下 AK 取得的行經路徑、觸發產生 AK 的三個時機點等等。最後分析換手過程時因整體訊息傳送所造成的網路負擔。

2.1 WiMAX 環境架構

根據[4]所描述的網路參考模型(network reference model)，如Figure 2-1所示，WiMAX整個環境由MS、NAP與NSP三個主要區塊所組成。實體(entity)與實體(entity)之間都有reference point (RP)所連接(如R1， R2， R3， …)。以下就針對NSP與NAP兩個區塊分別做介紹。

NSP由一個或多個CSN (connectivity service network)所組成，如Figure2-2所示，而每個CSN 包含AAA、DHCP Server等元件(component)。主要負責對用戶(subscriber)提供IP層的網路服務，其項目包含：

1) 對 MS 派送 IP address；
2) 提供 Internet 的網路存取服務；
3) 用戶的授權認證；
4) 建立 ASN 與 CSN 之間的通道(tunnel)等相關服務。

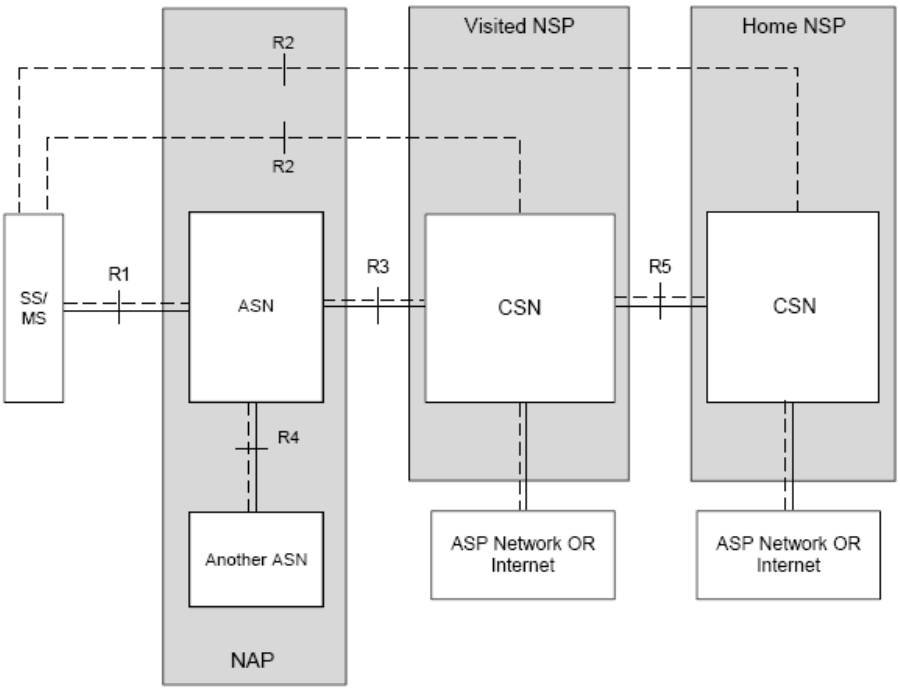


Figure 2-1 Network Reference Model

資料來源：[4]

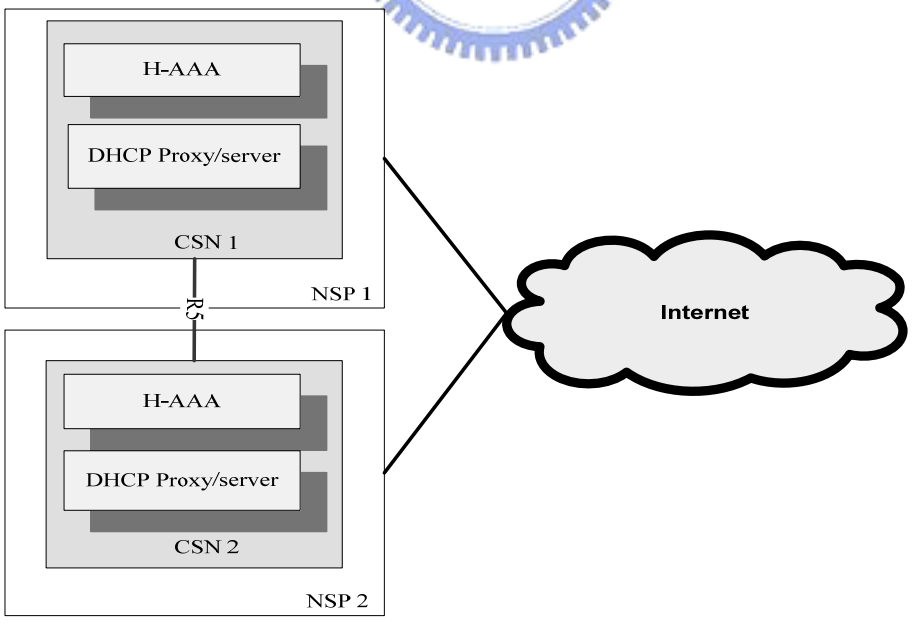


Figure2-2 NSP Reference Model

如Figure2-3所示，NAP由一個或多個ASN (access service network)所組成，爲電信

業者(operator)所規劃，擔任MS與NSP之間的溝通橋樑。ASN提供R1 與MS溝通，R3 與NSP溝通。ASN允許與多個NSP溝通，這僅看雙方合約如何簽定(license agreement)。ASN的組成元件包含有BS與ASN-GW。BS與BS之間透過R8 連結，ASN-GW與ASN-GW之間透過R4 連結，而BS與ASN-GW則透過R6 連結。不同的ASN之間 (inter-ASN)的溝通需透過ASN-GW來傳送。對於不同的NAP之間 (inter-NAP)的溝通，亦需透過ASN-GW傳送。根據[4]中對RP對安全性規定：

- **R2 (MS-CSN)**：MS 與 CSN 之間建立的通道(channel)**可能沒有安全性**；
- **R3 (ASN-CSN)**：ASN 與 CSN 之間建立的通道(channel)**可能沒有安全性**；
- **R4 (ASN-ASN)**：ASN 與 ASN 之間**有安全性**的通道(channel)；
- **R5 (CSN-CSN)**：CSN 與 CSN 之間建立的通道(channel)**可能沒有安全性**；
- **R6 (BS-ASNGW)**：BS 與 ASNGW 之間**有安全性**的通道(channel)；
- **R8 (BS-BS)**：BS 與 ASNGW 之間**有安全性**的通道(channel)。

本論文稍後的探討與分析，會對 reference point 的安全性來做考量。

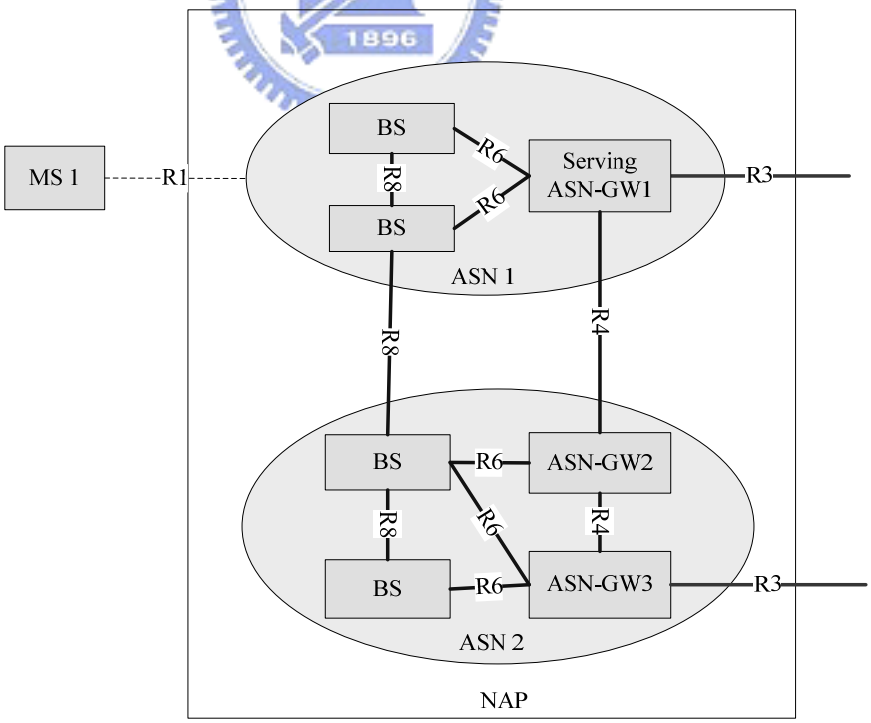


Figure2-3 NAP Reference Model

資料來源：[4]

2.2 WiMAX認證架構

2.2.1 MS端認證架構

IEEE802.16e[2]針對MS在無線傳輸的安全性裡定義了security sub-layer來提供隱密(privacy)、認證(authentication)與機密(confidentiality)等服務。而在security sub-layer裡包含了安全性的架構key management protocol (PKM)平台如Figure2-4所示，在PKM平台之上提供不同的認證機制，允許BS與MS之間做單向或雙向認證。IEEE802.16e提供兩種明確的認證機制 RSA與EAP。如之前所說，NWG已明確捨棄RSA機制。因此本論文只探討EAP認證機制。PKM的目的在於MS與BS之間建立一把共用的金鑰(shared secret)AK。利用AK爲加密資料(data)所需要的traffic encryption key (TEK)做一層編碼保護。

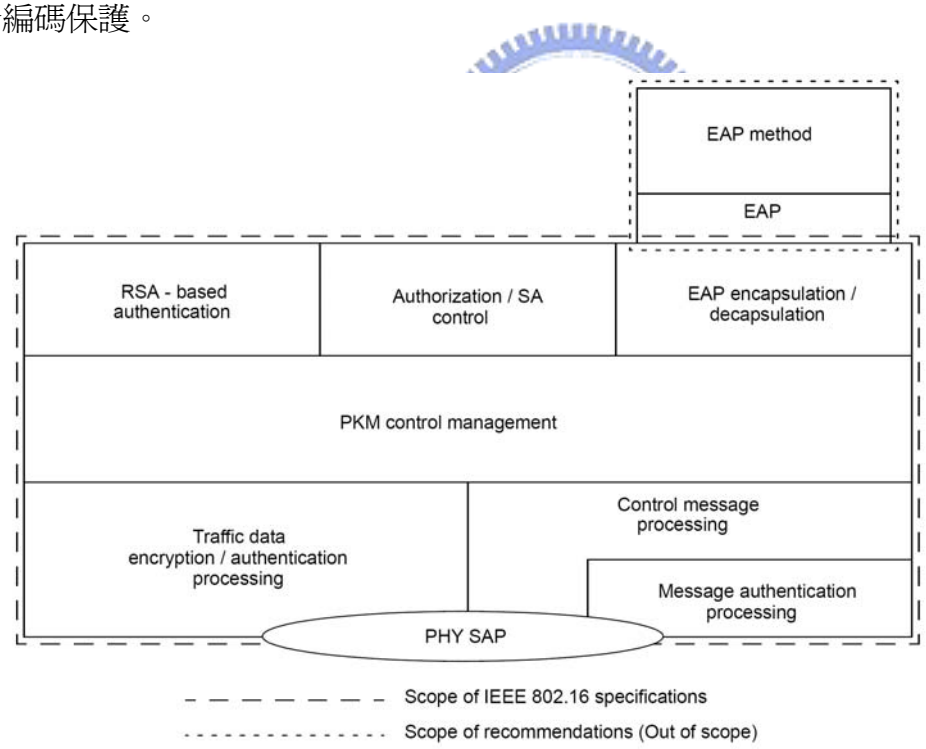


Figure2-4 Security Sub-layer

資料來源：[2]

2.2.2 Backhaul端認證架構

如Figure2-5.所示，MS爲一個supplicant，在要求允許進入WiMAX網路時會啓

動認證程序，透過EAP認證模式(以PKMv2 爲搭載工具)傳送認證封包。BS接收封包後轉送(relay)至authenticator(通常與ASN-GW擺放在一塊)，由authenticator負責傳送至指定的authentication server (AAA，如RADIUS server)，讓AAA 判斷supplicant是否爲合法的使用者。經由AAA確認後MS始得進入WiMAX網路。

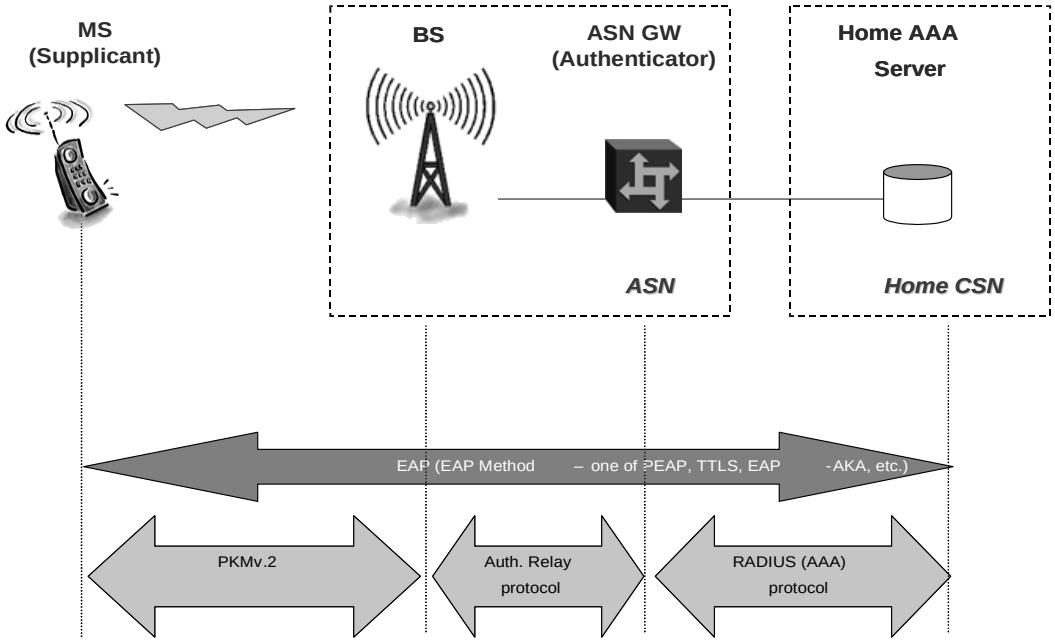


Figure2-5 WiMAX 認證架構.

2.2.3 Network entry中的認證程序

當MS欲登入WiMAX網路時(initial network entry)，首先傾聽BS發出廣播(broadcast)訊息。在MS聽到DL-MAP (downlink-map)訊息後，藉由分析(parsing)訊息內容可以取得 48-bit base station id (BSID)，BSID爲後來MS產生AK的必要參數(parameter)。MS收到DL-MAP之後，會發出Ranging Request (RNG-REQ)訊息給BS，其中RNG-REQ包含MS的MAC Address，也是後來產生AK所必須的參數。BS收到RNG-REQ訊息後若允許MS連線，則BS回傳Ranging Response (RNG-RSP)訊息給MS；其中RNG-RSP也包含BSID。待MS與BS透過ranging校正power和timing之後，MS發出SS Basic Capability Request (SBC-REQ)訊息給BS並詢問BS所能支援PKM

的版本與認證的模式。當MS收到BS回傳的SS Basic Capability Response (SBC-RSP)訊息，根據訊息內容確認BS支援PKMv2 且認證模式爲EAP模式後，MS才開始發送EAP-Start訊息，啓動 802.1X認證機制，如Figure2-6所示。

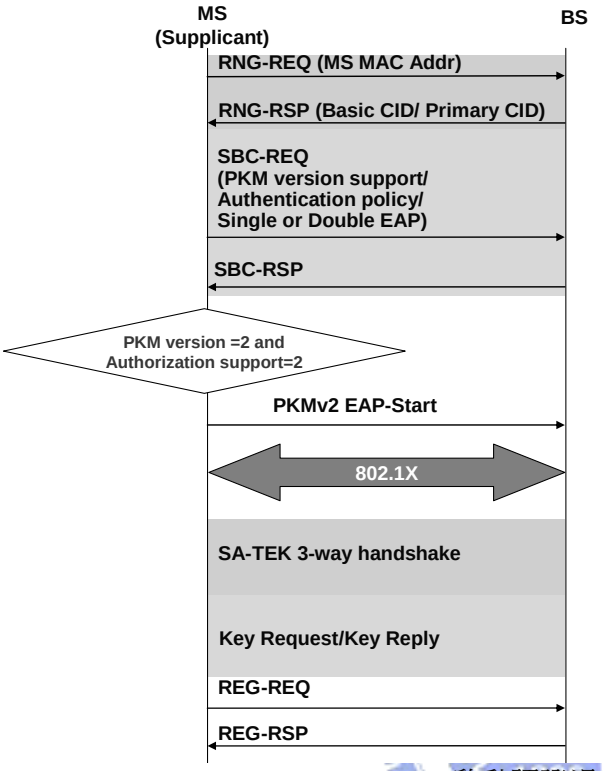


Figure2-6 MS 啓動認證過程

2.2.4 認證(Authentication)

MS欲登入WiMAX網路必須按照EAP認證程序(EAP Authentication)進行認證。參照Figure2-7流程圖(sequence model)詳述認證過程：

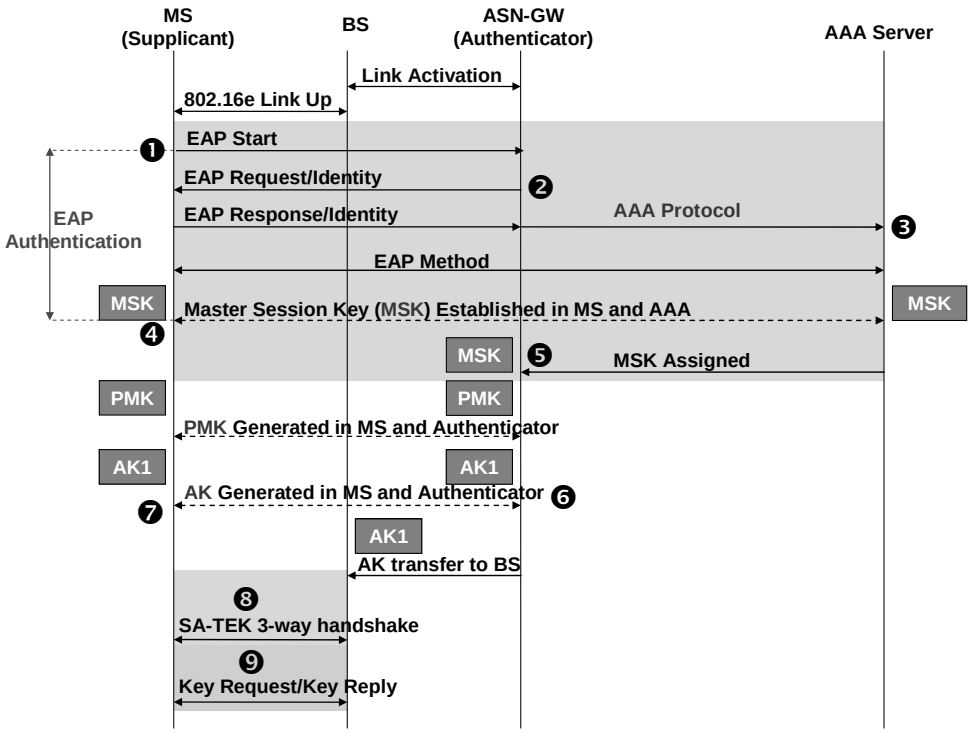


Figure2-7 MS 認證過程

1. supplicant (MS)傳送 PKMv2 EAP-Start 封包給正在爲 MS 提供服務的 BS (serving BS)，表示開始啓動認證程序。BS 收到後負責轉送給後端的 authenticator (ASN-GW)。
2. authenticator 透過 EAP-Request 訊息要求 MS 提出識別資料(identity)，識別資料爲 network access identifier (NAI)格式，不僅識別身分，亦可判斷認證模式(authentication mode)爲 user 或 device。
3. 當 authenticator 收到 MS 回應的 EAP Response/Identity 訊息後便封裝該訊息並透過 Access-Request 封包傳送給 AAA 伺服器。AAA 伺服器接收到 Access-Request 封包後，分析封包內容得知 supplicant 的身份且認證模式 (authentication mode)爲 user 或 device 後，提出建議的認證方法 (EAP method)並填入 EAP-Request，經由 Access-Challenge 封裝後回傳給 authenticator。在 supplicant 接收到 EAP-Request 訊息後可決定是否接受 AAA 建議的方法(EAP method)， supplicant 可以自行要求認證方法(EAP method)，要求 AAA 配合。認證方法有 EAP-MD5、EAP-TLS、EAP-TTLS、

EAP-SIM、EAP-AKA 等多種方法。待 supplicant 與 AAA 協商決定認證方法後開始進行認證。

4. supplicant 與 AAA 經進行多次認證程序後，若認證失敗，則停留一段 timeout 時間(heldWhile timer)後再重新認證。若認證成功，BS 會傳送 PKMv2 EAP Complete 封包，內容包含 EAP-Success 訊息給 MS，告知 MS 認證已經成功。AAA 伺服器與 supplicant 會各自產生一把金鑰 master session key (MSK)，認證過程結束，進入授權階段。

2.2.5 授權(Authorization)

認證程序完成之後接著開始啓動授權階段。如Figure2-7所示：

5. 當 AAA 伺服器在產生 MSK 之後會把 MSK 傳送給 authenticator
6. 在 authenticator 接收到 MSK 之後，authenticator 會經由 MSK 產生 pairwise master key (PMK)，再透過 PMK 產生 authentication key (AK)，AK 產生之後再傳送給 BS。
7. 在 authenticator 產生 key 的過程同時，supplicant 也會自行由 MSK 產生 PMK，再產生 AK，最終 MS 與 BS 各自獲得一把 AK。
8. 當 BS 與 MS 各自擁有一把 AK 之後，爲確保 MS 與 BS 共用同一把 AK，BS 會發送 PKMv2 SA-TEK-Challenge 封包給 MS，啓動 SA-TEK 3way handshake，藉以驗證的 AK 一致性。
9. 在確認 MS 與 BS 共用一把 AK 後，由 AK 產生一把金鑰 key encryption key (KEK)，負責加密 traffic encryption key (TEK)。TEK 爲 MS 與 BS 之間加密傳輸資料時所需的一把金鑰，由 MS 透過 key request 訊息向 BS 提出 TEK 需求，BS 收到之後隨機變數(random)產生 TEK，再透過 key reply 傳送給 MS。爲確保 TEK 不被攔截而破解，透過 KEK 加密，以確保 TEK 的安全。

2.2.6 Key 產生過程

Figure2-8描述key的產生及演進過程。經過上述EAP authentication認證(此處以single EAP爲例)成功後，透過pseudo random function產生出一把 512-bit的MSK (公式 1)；擷取(truncate)MSK的 160bits爲PMK，再由PMK帶入key distribution function (公式 2)產生AK。獲得AK之後根據MAC模式(mode)參照公式 3 或公式 4 產生一把KEK。

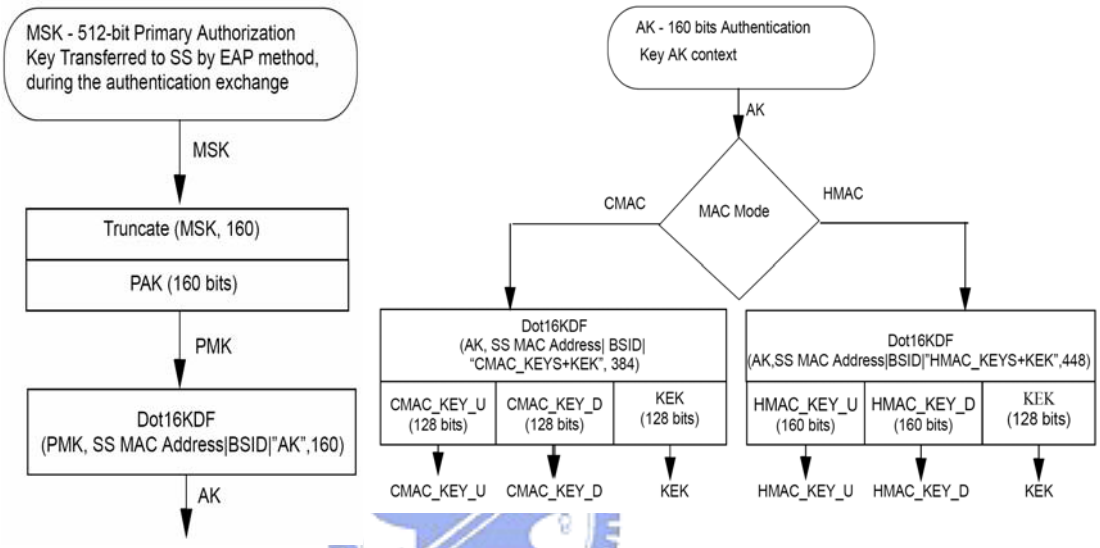


Figure2-8 Key hierarchy and derivations of 802.16e

資料來源：[2]

MSK=PRF(SecurityParameters.master_secret, "ttls keying material",

SecurityParameters.client_random + SecurityParameters.server_random) ([6]) 公式 1

AK=Dot16KDF(PMK, SS MAC Address | BSID | “AK”, 160) 公式 2

KEK=Dot16KDF(AK, SS MAC Address | BSID | “CMAC_KEYS+KEK”, 384) 公式 3

KEK=Dot16KDF(AK, SS MAC Address | BSID | “HMAC_KEYS+KEK”, 448) 公式 4

2.3 HO procedure

2.3.1 MS/BS initiated HO

MS 在一開始(initial network entry)與 serving BS 認證成功之後，若發現 Receive

Signal Strength Indicator(RSSI)、Carrier-to-Interference-and-Noise Ratio(CINR)過低或 Bit Error Rate (BER)、Packet Error Rate (PER)過高或其他因素超過原先制定的門檻(pre-provision)，則可由 MS 或 BS 觸發換手動作(handover)程序。

參照Figure2-9，在MS或BS決定啓動HO程序之前，MS首先會去聽serving BS定期發送的Neighbor Advertisement (MOB_NBR-ADV)訊息。透過MOB_NBR-ADV，MS可以知道：

1) Operator ID：等同於 NAP ID；
2) Neighbor BSID：serving BS 週遭有哪些相鄰的 BS(neighbor BS)；
3) Mobility features supported：哪些 neighbor BS 提供 handover 服務；
4) HO Process Optimization：哪些 neighbor BS 支援 HO 過程的最佳化。

MS 可以利用 MOB_SCN-REQ 向 serving BS 要求一段時間去與 neighbor BSs 做進一步的訊息交換。MS 在接收到 serving BS 回傳的 Scanning Interval Allocation Response(MOB_SCN-RSP)message 後，可以得知目前 neighbor BS 的 scanning type、scan duration、interleaving interval 等相關資訊，知道如何(how)與何時(when)跟 neighbor BS 溝通，以取得更精確的資訊。

MS 收集到 serving BS 週遭 neighbor BS 的相關資訊後，可以了解 neighbor BS 的目前狀態。因此，若由 MS 觸發 HO (MS initiated)，則 MS 傳送 MOB_MSHO-REQ 訊息給 BS。若由 BS 觸發 HO (BS initiated)，則 BS 傳送 MOB_BSHO-REQ 給 MS。甚至 BS 可以透過 Download Channel Descriptor (DCD) message 知會 MS，由 MS 傳送 MOB_MSHO-REQ 來啓動 HO 程序。

當 MS 選擇要與哪幾台 neighbor BS 聯絡時，MS 會將候選名單填入 MOB_MSHO-REQ，透過 MOB_MSHO-REQ message 訊息給 serving BS，由 serving BS 負責與後端(backhaul)溝通。待 MS 收到 serving BS 發送的 MOB_BSHO-RSP message，分析(parsing)封包裡的下列欄位可以瞭解周遭 BS 的目前狀態，包括：

1) Neighbor BSID：radio resource controller (RRC)建議HO的BS有哪些；
2) Service level prediction：MS可以從BS獲得哪些服務；

3) HO process optimization：neighbor BS提供哪些HO最佳化服務。

MS保有最後的決定權，在MS決定哪一台BS爲target BS後透過HO Indication (MOB_HO-IND) message，告知serving BS最終的決定，由serving BS負責通知target BS，MS也透過Ranging Request (RNG-REQ) message開始嘗試與target BS連接。

MS handover 時發出 RNG-REQ 給 target BS，若不需重新做競爭(initial ranging)，且 MS 欲連接的 target BS 需做認證授權服務，則 MS 發送 RNG-REQ 會帶有 HMAC 或 CMAC，此時 target BS 需要有原先 serving BS 的 AK 來驗證 MS 的身分，若身分驗證成功後 MS 與 target BS 得需要再重新取得一把新的 AK，作爲兩者之間的共同金鑰。

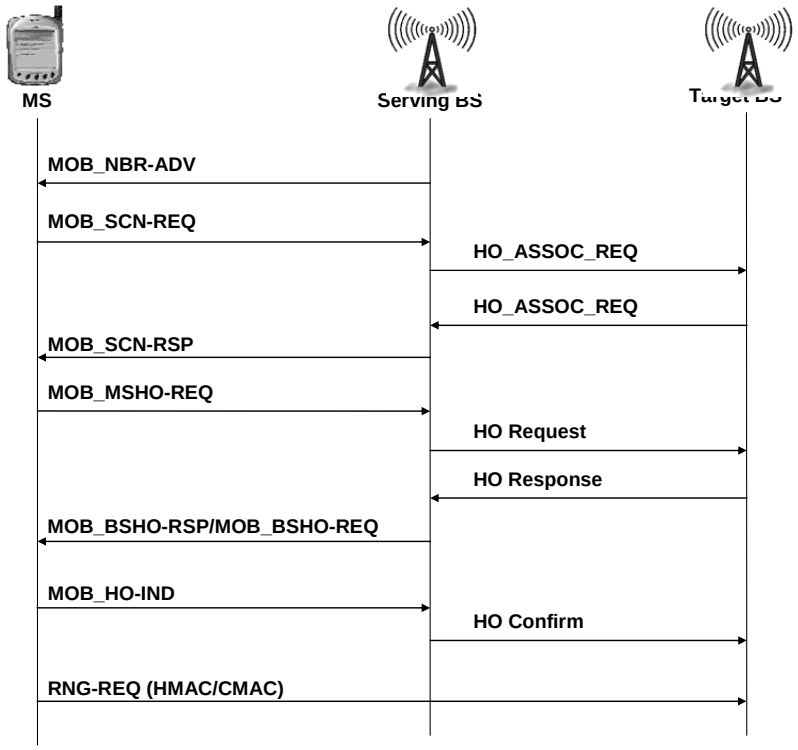


Figure2-9 802.16e HO procedure

資料來源：[4]

在介紹完前端(MS與BS)的認證授權過程後，接下來探討後端(backhaul)網路對於認證授權的處理方式與運作流程。[4]描述後端在處理HO過程時，有三種考慮的環境，接下來會針對不同的環境介紹封包的傳送流程。

2.3.2 Intra-ASN HO

[4]中描述當MS或BS啓動HO時，backhaul network端的認證流程如何運作。如Figure2-10 HO procedure in Intra-ASN model所示，在ASN的環境下，MS在一開始(network entry)與BS1 認證成功後，MS與BS1 會共用一把AK1，而當時爲BS1 處理EAP認證訊息並產生AK1 的authenticator稱爲anchor authenticator。當MS移動到BS2的覆蓋範圍而欲與BS2 聯繫時，BS1 同時傳送HO Request(表格 A-1)訊息給BS2，並提供MS的相關資訊。BS2 收到HO Request之後，若MS傳送帶有HMAC/CMAC的RNG-REQ給BS2 時，爲了能夠解析確認HMAC/CMAC的正確性，BS2 會送Context Request訊息給anchor authenticator，要求anchor authenticator提供MS當時在BS1 的AK Context (表格 A-5)，anchor authenticator會將有關於MS安全性的資料(AK Context)，透過Context Report (表格 A-3)訊息回傳給BS2。當MS handover 到target BS後，兩者之間因需要一把新的AK2，爲了加快HO的速度，[2]明白指示在NAP的環境底下不需要做re-authentication，而是利用anchor authenticator原先與MS認證成功所產生的PMK，爲target BS再產生一把新的AK2。因此當target BS發送AK Request訊息給anchor authenticator，要求提供一把新的AK2 時， anchor authenticator會由現有的PMK運算產生新的AK2 及相關安全性資料後，儲存至AK Context，透過AK Transfer封裝後回傳給target BS。值得注意的是，若ASN的涵蓋範圍很大，當MS持續的往前行而不斷做HO時(如Figure2-10中MS移動到BS3)，隨著BS與anchor authenticator距離的越拉越長，因anchor authenticator不會更換，造成兩者之間訊息傳送的延遲時間也隨距離變長，這對即時應用程式來說會有延遲反應。本論文稍後會針對這點提出一套解決方法。

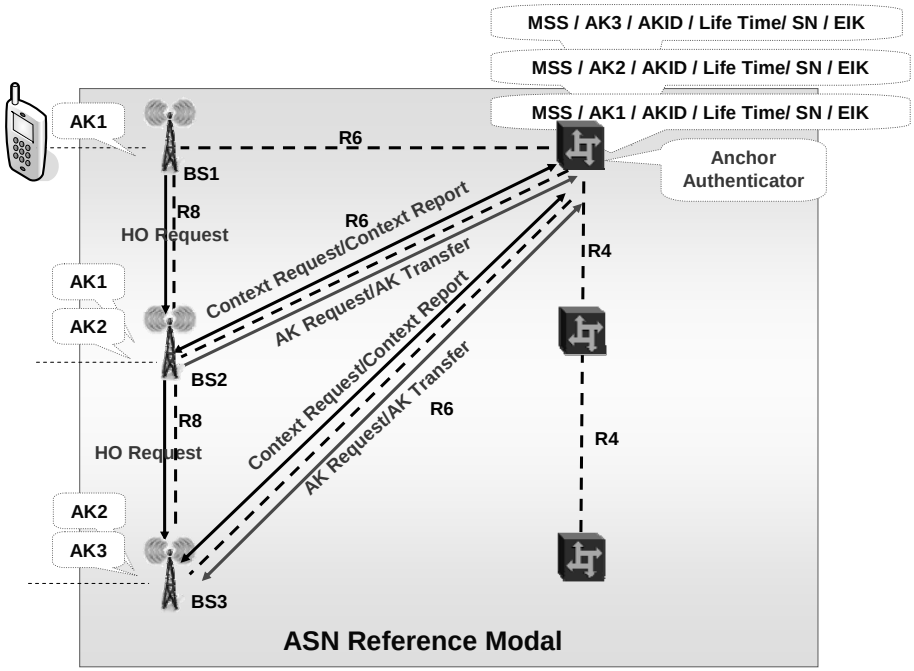


Figure2-10 HO procedure in Intra-ASN model

2.3.3 Inter-ASN HO

若MS在HO時所連接的target BS與serving BS跨越不同的ASN (Inter-ASN)，但還是屬於相同的NAP (Intra-NAP)時，如Figure2-11所示，MS在BS1 的覆蓋範圍移動至BS2 的覆蓋範圍時，與Intra-ASN不同的是，serving BS (BS1)無法直接傳送HO Request給target BS (BS2)，而是得由BS1 經由ASN-GW1、ASN-GW2 最後再傳至target BS (BS2)。另外，anchor authenticator並不因跨越不同的ASN而改變，因此還是由原先的authenticator爲anchor authenticator。另外，target BS爲取得MS原先在BS1 的AK Context，發出Context Request訊息給anchor authenticator，其行經路線爲BS2→ASN-GW2→ASN-GW1。anchor authenticator在收到訊息後將MS舊有的AK Context資訊透過Context Report訊息，經由ASN-GW1→ASN-GW2 回傳到BS2。同樣的，爲取得屬於MS與target BS之間的一把新的且共用的AK，target BS會發送AK Request訊息給anchor authenticator，其行經路線爲BS2→ASN-GW2→ASN-GW1。待anchor authenticator計算出AK後填入AK Context欄位，借由AK Transfer封裝後經ASN-GW1→ASN-GW2 最後傳送給BS2。

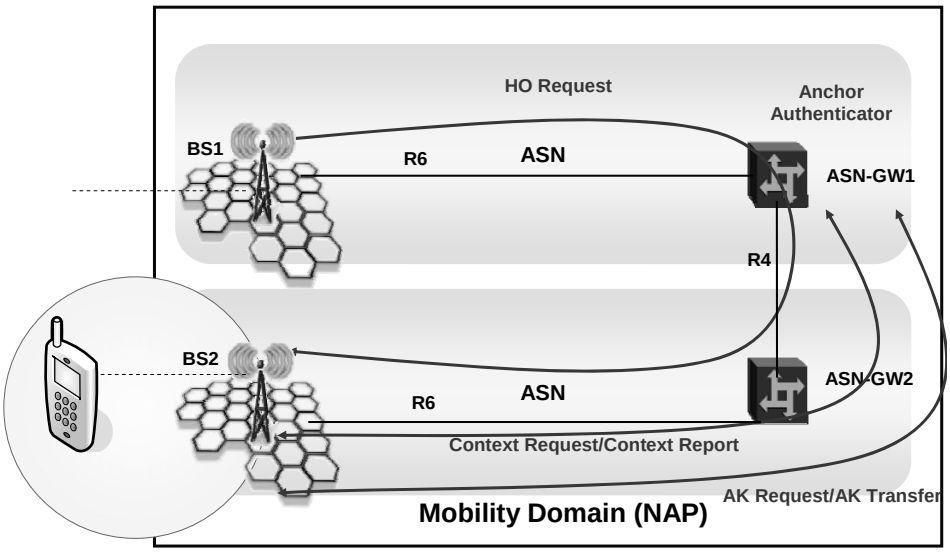


Figure2-11 HO procedure in Inter-ASN model

2.3.4 Inter-NAP HO

如Figure2-12，若MS在HO時所連接的target BS與serving BS是跨越不同的NAP (mobility domain)，與前面兩者不同的是，不同的NAP爲不同的operator，兩者之間可能沒有信任關係(depend on license agreement)，而且[4]僅針對mobility domain下的HO提出說明。另外，在不同的NAP之間的reference point (RP4)沒有安全性的保障。因此當MS由BS1 移動至BS2 後，無法由之前的anchor authenticator (此處爲ASN-GW1)爲BS2 產生一把AK。於是在BS1 傳送HO Request給BS2 時 (經由BS1→ASN-GW1→ASN-GW2→BS2)，BS2 經判斷爲不同的NAPID，決定重新做full authentication。

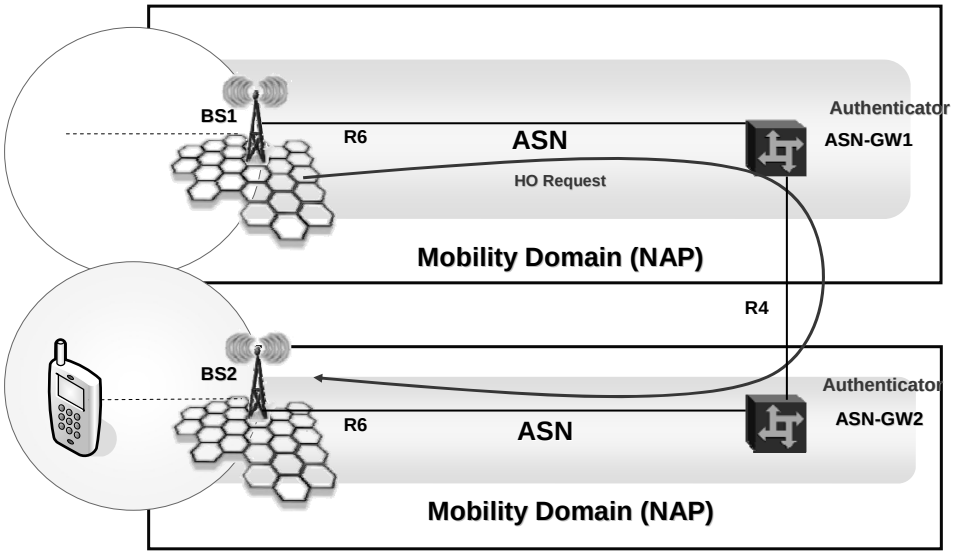


Figure2-12 HO procedure in Inter-NAP model

2.3.5 AK在HO時產生的時間點

前面的章節介紹完MS端的認證處理方式以及backhaul端對於認證的運作處理模式後，接下來要探討的是觸發AK產生的時間點，執行AK Assignment流程。NWG裡[4]提出 3 種觸發AK Assignment的時間點(Figure 2-13)：

1) **MS發送MOB_MSHO-REQ給serving BS**：爲使得MS在handover能達到無接縫(seamless)的效果，讓MS移動到target BS時不需因backhaul端的一連串處理過程過於冗長。因此[4]提出hackhaul端允許AK的產生流程越早進行越好。所以當MS發出MOB_MSHO-REQ時，在MS尚未決定target BS(只有建議名單時)之前，即要求各個候選的BS (candidate target BSs)開始產生新的AK。因此各個候選的BS會向anchor authenticator提出要AK的需求(request)，這加重了anchor authenticator的負擔，因爲anchor authenticator幫助可能不是最終target BS的候選者計算AK (畢竟只有target BS的AK有用)。這也加重了 candidate target BSs 爲了可能不會進來涵蓋範圍的MS去產生AK而增加額外的負擔。

2) **MS 發送 MOB_MSHO-IND 給 serving BS**：當 MS 決定 target BS 後，發出

MOB_HO-IND 訊息給 serving BS，由 serving BS 負責通知 target BS 去產生 AK Assignment。相較於前一項 AK Assignment 的時機點，anchor authenticator 不會因爲替 candidate target BSs 產生 AK 而增加負擔，candidate target BSs 也不須爲 MS 產生 AK 而增加 overhead。

3) **MS發送RNG-REQ給target BS**：[4]允許MS移動到target BS後才要求AK Assignment，但這種情形有可能導致handover的延遲時間會比上述兩者還長，因爲前兩者是由servering BS還在服務MS的情況下由serving BS負責通知target BS去提出AK需求(request)，target BS在還沒服務MS之前可以有充裕的時間去申請新的AK，所以當MS發出RNG-REQ給target BS後，target BS就已經擁有新的AK了；但第三種情況爲因MS欲連結target BS時才由target BS發出AK Assignment需求，MS必須等待target BS獲得新的AK後MS才可以繼續往下執行，這會導致換手的延遲時間拉長。因此本論文稍後提出的解決方案，將不會在這種狀況下要求AK Assignment。

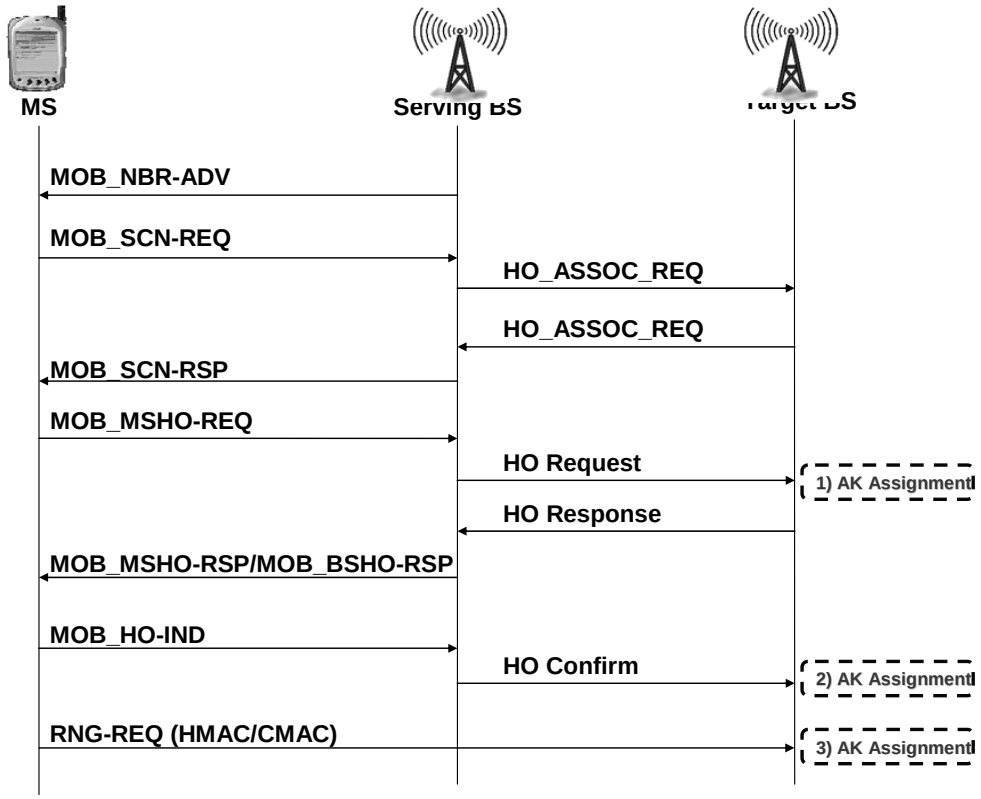


Figure 2-13 AK 產生的時間點

2.4 AK在HO時的產生流程

經過前面2.3.5介紹MS在handover過程中AK產生的三個時機點後，本節針對這三種時機點詳述完整的訊息傳送過程：

1) 第一種情形參照Figure 2-14描述MS在發出MOB_MOB-REQ訊息後，其中訊息欄位包含MS MAC Address與可能的相鄰BS連結的候選名單(candidate target BSs，此例爲neighbor BS1 與neighbor BS2)。待serving BS收到之後，透過HO_Request (表格 A-1)封包傳遞給neighbor BS1 和neighbor BS2；此時neighbor BS1 和neighbor BS2 可以選擇在這準備階段(preparation phase)傳送Context Request (表格 A-2)給anchor authenticator，要求anchor authenticator提供MS在與serving BS連結時所使用的AK Context。Context Request若選擇不在這個時機點發出，則必須等到行動階段(action phase)才能發送訊息。當neighbor BS1 和 neighborBS2 接收到anchor authenticator所發出的Context Report (表格 A-3)之後，neighbor BS1 再透過 AK Request向anchor authenticator要求MS與neighbor BS1 之間的一把新的AK2，而neighbor BS2 也向anchor authenticator要求一把MS與neighbor BS2 之間的一把新的AK3。anchor authenticator在收到AK Request訊息後，判斷是否仍保有該MS的PMK。若有，則anchor authenticator將新的AK2 及AK3 填入AK Context，經AK Transfer 封裝後各自回傳給 neighbor BS1 和neighbor BS2，完成AK的產生過程。根據上述的流程，可以定義出**AK Assignment機制包含 Context Request**、Context Report、AK Request 和 AK Transfer。

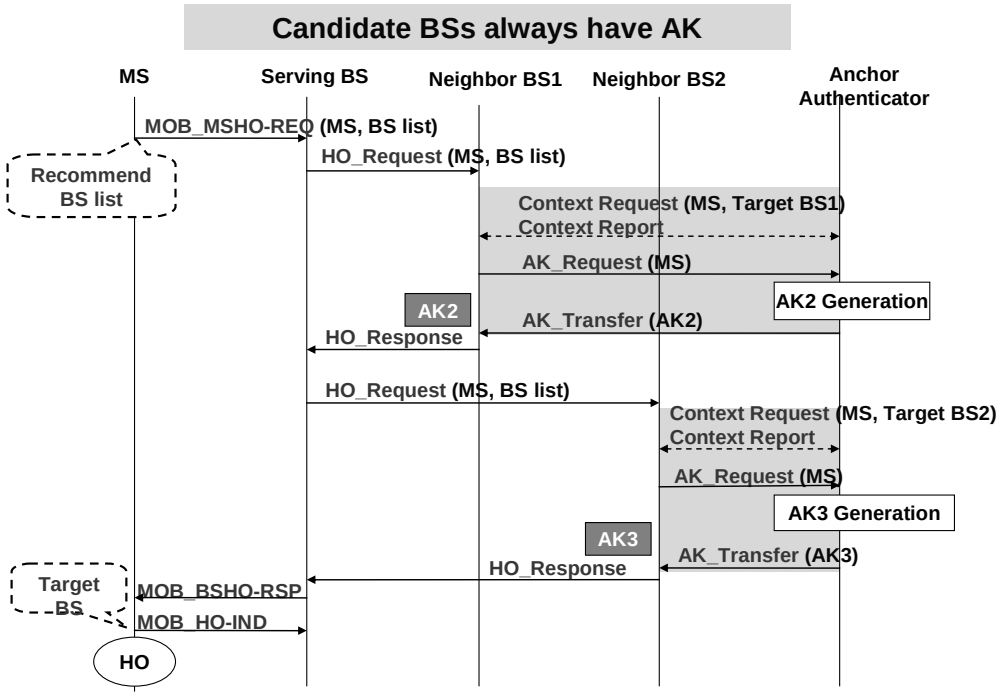


Figure 2-14 AK Triggered by MOB_MSHO-REQ

2) 第二種情形爲 MS 決定 target BS 之後才發出 MOB_HO-IND 訊息，對於第一種情形在獲得 AK 失敗後還有機會再次求得 AK。此時 serving BS 傳送 HO Confirm 訊息給 target BS，當 target BS 接收到確認訊息後，首先回傳 HO Ack 給 serving BS，通知 serving BS 已經收到訊息了。target BS 接下來跟前面的情形一樣執行 AK Assignment，可選擇性的透過 Context Request 向 anchor authenticator 要求原先舊的 AK 後，再透過 AK_Request 要求一把新的 AK2。

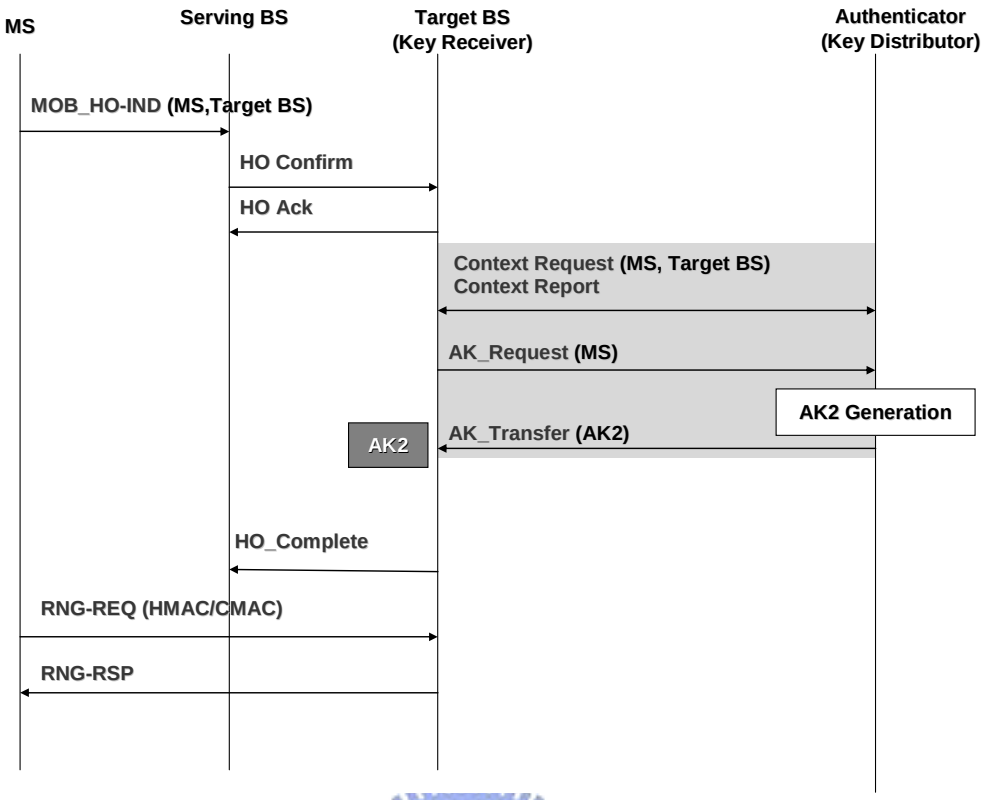


Figure 2-15 AK Triggered by MOB_HO-IND

3) 在前面兩種情形在獲得AK均失敗得情況下，[4]還提供第三種情形，爲MS移動到target BS後發送RNG-REG訊息時，target BS才開始去要求取得AK2 (Figure 2-16)。因MS發送的RNG-REQ帶有HMAC/CMAC，target BS必須要有能力能夠解開，因此target BS必須立刻發送Context Request訊息給anchor authenticator，要求取得MS之前與serving BS共用的AK Context，在這之後target BS還得需要向anchor authenticator取得介於MS與target BS之間新的AK Context。

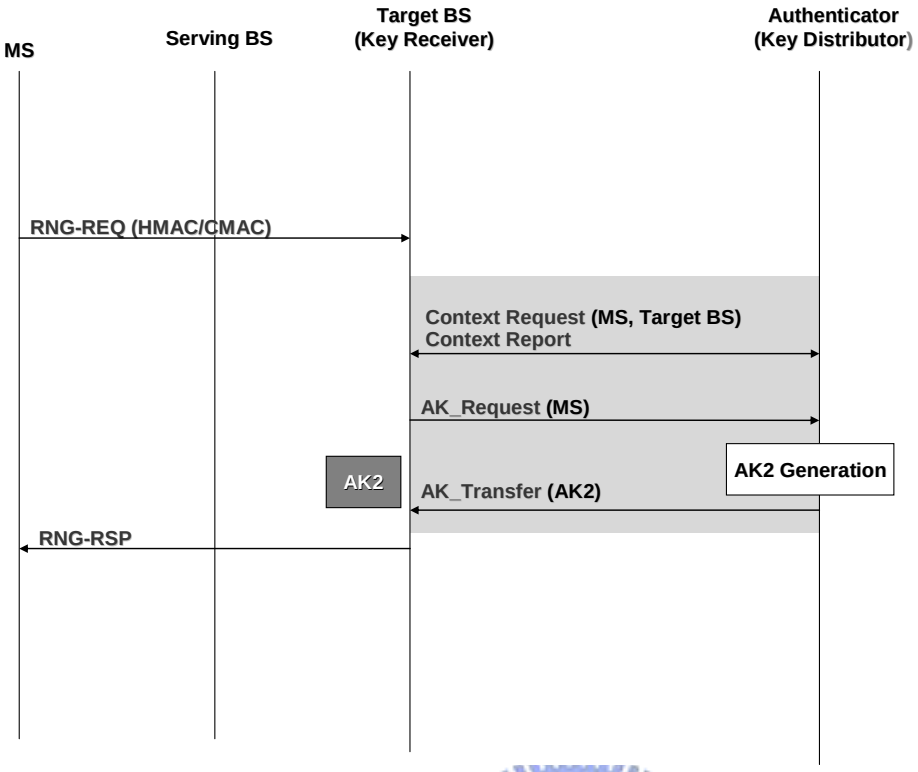


Figure 2-16 AK Triggered by RNG-REQ

分析以上的三種情形之所以能產生新的 AK，必須建立在 PMK 已經存在的前提下才能成立，若 PMK 不存在則必須重新做 authentication (initiating re-authentication)。同樣的，當 MS 移動到另一個 NAP (mobility domain)底下的 target BS，則會因原先的 anchor authenticator 無法使用，亦得重新執行 re-authentication。

另外觀察的是，無論是上述哪一種情形，取得舊有或新的 AK 皆需要有 AK Assignment 訊息 (Context Request、Context Report、AK Request、AK Transfer)。尤其是第一種情形，在尚未確定 target BS 時即要求所有可能的 candidate target BSs 各自向 anchor authenticator 要求一把 AK，無疑是加重 backhaul 網路及 anchor authenticator 的負擔。因此本論文在下一節，提出新的方法來解決這些問題。

第 3 章

Distributed security mechanism

經由第二章描述 WiMAX 的架構下的整個認證授權程序，並分析 MS 在 handover 時的 AK 的產生過程及所需要花費的負載(loads)後，本章節提出本論文的觀點並提供解決方法來減少 handover 中因 AK 產生的過程而導致延遲時間及增加 backhaul 端的網路負擔。

3.1 節中提出本論文的構想；3.2 節提出分析論點。

3.1 分散式AK 傳送方式

爲解決前面所描述 handover 所造成 backhaul 端的網路負擔，本論文提出兩個論點：

1) 將原先在 MS 與 BS 之間共用 AK 的範圍擴大爲 MS 與 NAP (network access provider)之間共用的一把 AK。若 serving BS 與 target BS 在 mobility domain 範圍下共用一把 AK 後，則 anchor authenticator 不需要再爲 MS handover 過程中重新計算一把 AK，藉以減少 anchor authenticator 的運算負擔(computation loads)。

2) 既然 MS 在 NAP 的範圍下所有的 AK Context 都相同，接下來的考量點爲：

   i) 誰負責傳送 AK Context；

   ii) 誰可以收到 AK Context；

   iii) 什麼時機點傳送；

   iv) 以及透過什麼封包傳送。

   本論文提出論述爲：既然serving BS已有MS的AK Context資料，且R6、R8 爲安全的通道，就讓serving BS取代anchor authenticator，透過HO Request (表格 A-7)訊息將MS的AK Context (表格 A-5)傳送給candidate target BSs (Figure 3-1 Propose HO procedure)，這樣有幾點好處：

a) serving BS 傳送訊息給 candidate target BSs 的距離會比原先 WiMAX 設計由 anchor authenticator 傳送訊息給 candidate target BSs 的距離還短。

b) 因爲MS在NAP (mobility domain)範圍內的AK在lifetime時間之內不會變更，因此可以減少candidate target BSs或target BS與anchor authenticator之間傳送 Context Request (表格 A-2)、Context Report (表格 A-3)、

AK Request、AK Transfer訊息，也因此會減少網路後端的負擔 (traffic loads)。

c) Candidate target BSs 不需要爲找尋 anchor authenticator 而重新建立 BS 與 anchor authenticator 之間的路徑。

所以若觸發啓動handover過程時，亦即MS發出MOB_MSHO-REQ給serving BS 時或BS發出MOB_BSHO-REQ訊息給MS時(Figure 3-1)，由serving BS根據MOB_MSHO-REQ或MOB_BSHO-REQ裡所建議的candidate target BSs，負責透過HO_Request發送AK Context訊息給這些BSs，而這些candidate target BSs則不再透過anchor authenticator來取得。

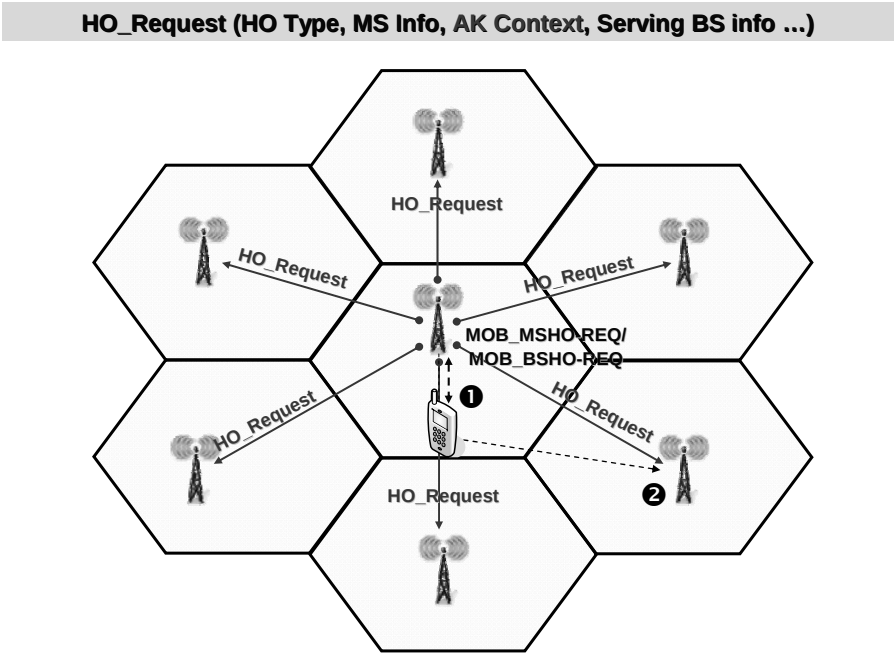


Figure 3-1 Propose HO procedure

3.2 論點分析

3.2.1 流程分析

根據3.1所提出的論點，以Figure 2-14爲例，重新解釋修改過後的系統運作流程。由圖(Figure 3-2)可知：

1) MS 與 serving BS 連結時已經各存有一把共享的 AK1，當 handover 發生時，則 MS 傳送 MOB_MSHO-REQ 訊息裡夾帶著包含 candidate target BSs 的名單(MS initiated)；亦或是 BS 發出 MOB_BSHO-REQ 封包裡夾帶 candidate target BSs 通知 MS 關於相鄰 BS 的目前狀態(BS initiated)。

2) serving BS接收到MS傳送的訊息後透過HO_Request（包含MS MAC Address、 target BS info等)，將這些做HO時所必須要的相關資料，根據target BS info欄位所提供的建議名單(one or more)傳送出去，因此相鄰的BS1 與BS2 在收到訊息後可以獲得MS的資訊。原先[4]中描述candidate target BSs收到HO Request訊息後會向anchor authenticator要求原先MS與serving BS之間的AK Context (透過Context Request)以及要求爲MS與target BS之間產生新的AK Context (透過AK Request)。而本論文所提出的方法是讓AK Context在NAP (mobility domain)範圍下不會改變，因此省略了要求AK Context的步驟。所以authenticator在handover過程裡不參與其中，也降低了後端網路及authenticator的負擔。

3) 當MS移動到target BS後，若MS在RNG-REQ不需重新競爭(initial ranging)的情況下，RNG-REQ 會夾帶 HMAC/CMAC 傳送給 target BS，target BS 可以藉由 HMAC/CMAC 驗證是否與 MS 所擁有相同的 AK (確保 AK 的一致性) ，若 target BS 無法確定 RNG-REQ，則啓動 ”Un-secure location update”流程，清除 MS 的相關資料。

4) MS在與target BS連接時，若MS傳送RNG-REQ需做重新競爭，則MS與BS會透過SA-TEK 3way handshake階段確認AK Context的一致性(原先[2]設計SA-TEK 3way handshake的目的除了爲驗證新的AK外還有傳送security association，因此流程不可省略)。

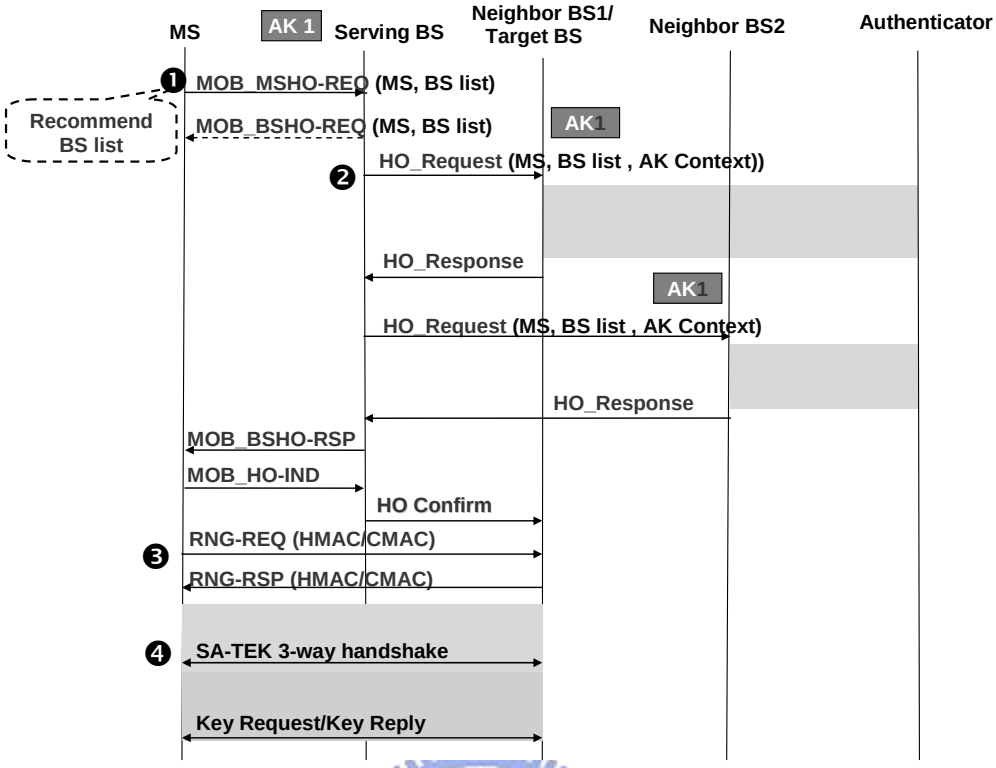


Figure 3-2 Proposed AK Transferred procedure

3.2.2 欄位分析

對於前端網路來說(MS與BS)，由於本論文將AK的涵蓋範圍由原先MS與BS之間的關係，擴大爲MS與NAP之間的關係，因此AK的產生公式(0)，亦得更新。原先的BSID參數，必須更改爲NAPID，因此需要更改的公式在修改後如下：

AK=Dot16KDF(PMK, SS MAC Address | NAPID | “AK”, 160)

AKID=Dot16KDF(AK, AK SN|SS MAC Address |NAPID|"AK", 64)

NAPID 的獲得方式與 BSID 相同；BSID 可由 DL-MAP 裡取得 48-bits 的識別號(identifier)，而 NAPID 爲 BSID 的前 24-bits(MSB)，因此不需要爲求得 NAPID 而增加額外的負擔。

針對後端網路(backhaul)來說，[5]中描述：

1) HO Request (表格 A-1)在intra ASN是不帶有AK Context欄位。
2) 經由ASN-GW發出的HO Request (表格 A-8)則可選擇性(option)帶有AK Context。

3) 若ASN-GW之間傳送的HO Request (表格 A-8)，欄位裡不含有authenticator id與AK Context欄位則表示MS所在的serving ASN與 authenticator ASN是屬於相同的ASN。

本論文則修訂爲：

1) 在 intra ASN 所傳送的 HO Request 必須(must)增加 AK Context 欄位。

2) 經由 ASN-GW 之間傳送的 HO Request，必須(must)帶有 AK Context 欄位。

3) 既然 ASN-GW 之間傳送 HO Request 時 AK Context 爲必要輸入的欄位，因此 HO Request 裡不包含 authenticator id 才表示 serving ASN 與 authenticator ASN 爲同一 ASN。

3.2.3 環境分析

決定流程之後，接下來得考慮的是環境，環境的差異會導致訊息封包傳送的行經路徑有所不同。前面2.3裡描述了WiMAX的三種環境：Intra-ASN、Inter-ASN與Inter-NAP。在Intra-ASN與Inter-ASN的情況下，MS在handover過程由於anchor authenticator不會改變(參照2.3.2與2.3.3)因此適用於本論文的解決方案；至於Inter-NAP，由於跨越不同的NAP (mobility domain)，NAP與NAP之間並不一定有信賴關係或合約關係，因此在inter-NAP的情況下serving BS與target BS無法共用anchor authenticator。此外，[4]明白指示PMK不能分享給不同的authenticator，當MS更換不同的anchor authenticator時，原先的PMK是無法再被利用。因此當跨越不同的NAP時，得重新做authentication(initiating re-authentication)。

3.2.4 AK Context維護

由於 serving BS 在 MS handover 的過程中將 AK 的 Context 透過 HO Request 傳送給 candidate target BSs，因此接收到的 BS 在收到訊息後立即判斷下列事項：

1) Candidate target BSs根據HO Request (表格 A-7)訊息裡的Serving BS Info欄位判斷serving BS與自己是否在同一個NAP底下。若不是的話，表示MS跨越不同的

NAP，則需做full-authentication；若是的話，則進行步驟二。

2) Candidate target BSs 根據 MS 的 MAC Address 判斷是否曾經保留該 MS 的 AK Context，沒有的話就儲存，有的話則根據 AK sequence number 來決定最新資訊並取代原先的資料。藉以保持 AK Context 爲最新的狀態。

3) Candidate target BSs 會自行判斷 AK 的生命週期(lifetime)；若超過 AK 的生命週期則去掉 MS 的相關資訊。

3.2.5 安全性分析

本論文提出的解決方案，除了希望能減輕 WiMAX 網路負擔，並減少 handover 的延遲時間，安全性也是重要考量因素；唯有在安全性的環境下加速 handover 的效率才有意義。因此提出三個論述，來引證安全性的無虞。

1) MS 一開始(initial network entry)與 serving BS 做 full-authentication 時，由於與 AAA 的認證授權成功，才有產生從 MSK、PMK 到 AK，MS 才會與 serving BS 產生信賴關係。因此 MS 與 serving BS 之間的信賴關係可以說是由 AAA 所建立出來的。此外爲確保 R4、R6、R8 爲安全的 channel，理論上 BS 在 power on 時會先與 ASN-GW 認證。因此在 NAP 內，考量 BS 的安全無虞後，AK Context 存在哪個認證過後的 BS 並不影響安全性。

2) 根據本論文提出 AK 的公式：

AK=Dot16KDF(PMK, SS MAC Address | NAPID | “AK”, 160)

可以看出，除了 PMK 參數之外，其餘的輸入參數皆爲明文(plaintext)，任何人都可以得到。所以只要在 authenticator 的 PMK 不被破解，AK 自然安全。此外，當 MS 在 handover 過程中與 target BS 執行 RNG-REQ(包含 HMAC/CMAC)與 SA-TEK 3way handshake 時，都會驗證 AK，因此可以確保 AK 的正確性，防止 servign BS 傳送錯誤或過期的 AK Context。

3) 參考 [2] 中描述 Macro-diversity Handoff (MDHO) 與 Fast BS Switching (FBSS)，當MS要做handover時，可由週遭的BS協助MS，加快MS handover

的速度，而要週遭BS的幫助，前提是必須要周圍的BS擁有MS的相關資訊(context)，其中包括authentication key和 encryption keys。由此可知IEEE802.16e允許週遭的BS擁有MS的安全性資料。同樣地，本論文亦只允許candidate target BSs擁有MS的AK Context，因此本論文提出的解決方案符合在IEEE802.16e的設計精神。

第 4 章
偵測HO延遲時間

本論文所提出的方法較優於原先IEEE802.16e與WiMAX Forum所制定方式的項目如下：

1) 減少 candidate target BSs 爲取得 AK Context 而增加的工作量；

2) 減少 anchor authenticator 爲計算 AK 所造成的負擔 (computation loads)；

3) 減少 backhaul 端網路的負擔 (traffic loads)。

但卻也有增加額外的負擔：

1) Serving BS 傳送 HO Request 必須增加 AK Context (119KB)的欄位；

2) Auchor authenticator 記載 AK Context 的記憶體空間轉嫁到各個 candidate target BSs。

本論文的研究重點爲加速換手的速度，因此實驗重點將著重在換手時如何在不失安全性的情況下節省步驟來加速 handover。在做實驗之前，首先需瞭解本論文的實驗模型(model)。分兩部分來說明：第一個部份爲 ASN 內部的功能架構(functional view)，第二爲網路架構。得先確定功能架構後才能決定網路架構。接下來先針對這兩部份來做說明。

4.1 Function View

首先對於功能架構而言，本實驗對 ASN 的 functional view 是以業界普遍使用的 profile C 爲 base。相較於 profile B 將 ASN 整合在一起(包含 ASN GW、BS、Authenticator 等)，profile A 與 profile C 則將 ASN GW 與 BS 分開，而且 authenticator 擺放在 ASN GW。Profile A 是將 handover 的處理程序交由 ANN GW 負責統籌決策，BS 只負責轉送功能；Profile C 則是由 BS 負責處理 handover 的程序，ASN GW 僅負責轉送功能 (relay)，使用 Profile C 好處則是 BS 可以直接決策換手動作，不須經由與 ASN GW 協商而增加額外機制。

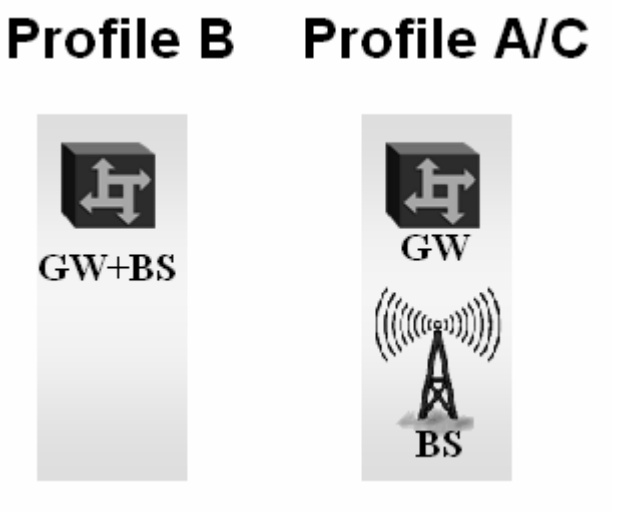


Figure 4-1 ASN Profile
資料來源：[4]

4.2 網路架構

另外在網路架構部分，是以[7]爲model base。本章節會先介紹[7]所提出網路架構及建立的分析模型(model)，然後再將WiMAX的環境導入模型後進行分析實驗。

4.2.1 ASN model

Figure 4-2爲ASN cell network的網路架構。在ASN內每個BS所涵蓋範圍爲一個cell，而cell內的數字表示爲階層(*l*-subarea cluster)。中心爲 0 階；爲authenticator與ASN GW所擺放的位置。其次爲 1 階、2 階、3 階以此類推。而MS在ASN環境裡的任一serving BS範圍下，移到周圍BS的機率爲 1/6。

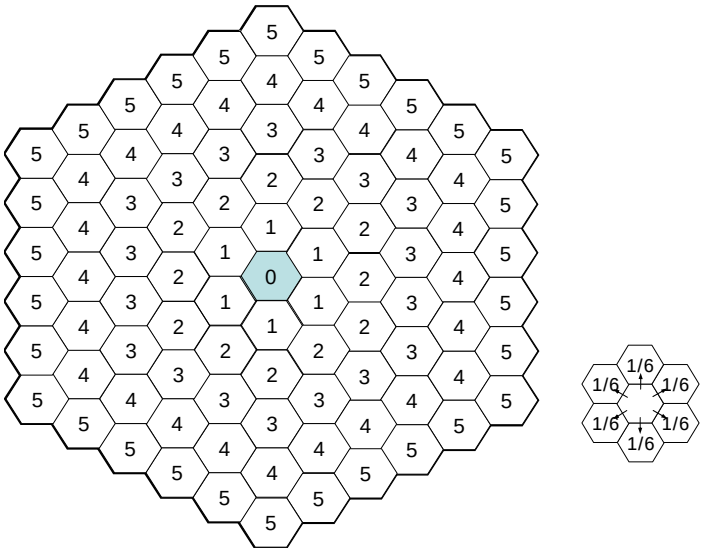


Figure 4-2 ASN Cell Network

資料來源：[7]

根據[7]所描述，若將ASN由三條線切開，分成六等分後，使用(*x*, *y*)區分每個等分內座標位置，如Figure 4-3所示，其中*x*仍表示爲階層(subarea- *x*)，*y*則表示爲type，與*x*一樣均由 0 開始算起，因此標記黑點的座標會是相同。所以既然每個等分的條件相同，只需討論其中一個等分即可(灰階部分)。

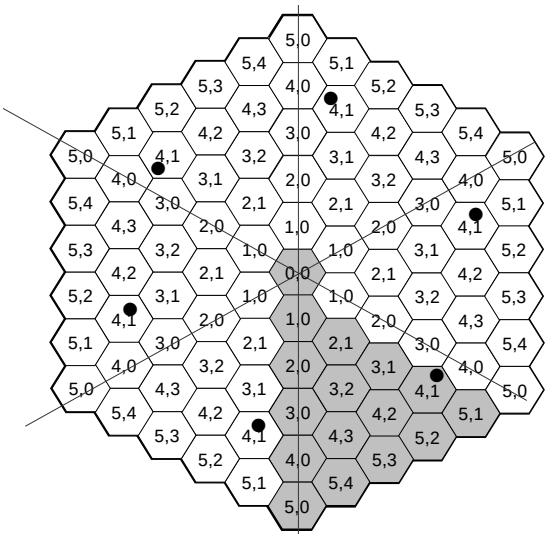


Figure 4-3 type classification

資料來源：[7]

觀察Figure 4-3，MS從座標(0,0)移動到(1,0)的機率爲 1，反觀MS的位置從座標 (1,0) 移動到(0,0)的機率爲 1/6，以此類推，則可推得以下的狀態圖(state diagram)，見Figure 4-4。

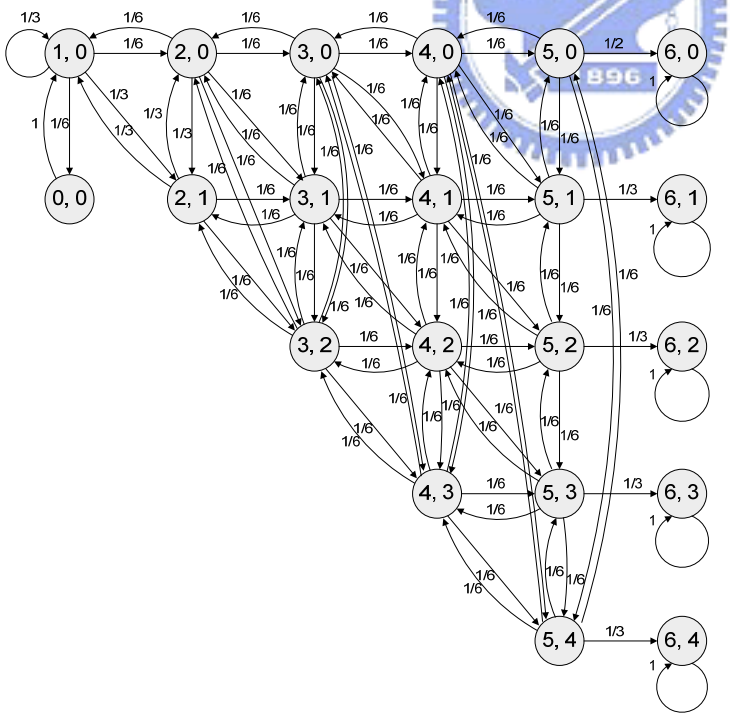


Figure 4-4 State Diagram for a 6-subarea Cluster

資料來源：[7]

接下來討論 MS 在任一個 serving BS 的 cell 裡(x, y)，經換手多個 BS 後跨出 ASN 的機率爲何？MS 在 ASN 內的 BS 座標爲(x, y)，其中 $0 \leq x < l$，$0 \leq y < x-1$。當 MS 移動到下一個 BS 的座標爲(x', y')，其機率表示法爲 $P_{(x,y),(x',y')}$。因此可以設定 MS 從(l -1, j)的座標移動到(l, j)而跨出 ASN，此時 $0 \leq j < l-1$，其機率表示法爲 $P_{(l\text{-}1,\,j),(l,\,j)}$。設定 $S(n)$表示在 l -subarea cluster 底下 MS 可隨機移動的 state 數。因此：

$$S(l) = \begin{cases} 2, & l = 1 \\ \dfrac{l(l+1)}{2}, & l > 1 \end{cases}$$

另外，以Figure 4-3爲例，在ASN內MS隨機移動的機率P = ($P_{(x,y),(x',y')}$)，用$S(l)\times S(l)$ matrix來表示爲：

$$\mathrm{P} = \begin{Bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1/6 & 1/3 & 1/6 & 1/3 & \cdots & 0 & 0 \\ 0 & 1/6 & 0 & 1/3 & \cdots & 0 & 0 \\ 0 & 1/3 & 1/3 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{Bmatrix}_{S(n)\times S(n)}$$

其中橫軸及縱軸的順序依序爲(0,0)，(1,0)，(2,0)，(2,1)，(3,0)，(3,1)，…，(6,3)。

$\mathrm{P}^{(k)}$ 表示 MS 移動 k 個步驟後的機率矩陣：

$$\mathrm{P}^{(k)} = \begin{cases} \mathrm{P}, & k = 1 \\ \mathrm{P} \times \mathrm{P}^{(k\text{-}1)}, & k > 1 \end{cases} \qquad (1)$$

其中， $p^{(k)}_{(x,y),(x',y')}$ 表示 MS 在座標(x, y)經過 k 個步驟後移動到座標(x', y')的機率。因此，MS 剛好在第 k 個步驟跨出 ASN 的機率可以表示如下：

$$p_{k,\,(x,y),(l,j)} = \begin{cases} p_{(x,y),(l,j)}, & k = 1 \\ p^{(k)}_{(x,y),(l,j)} - p^{(k\text{-}1)}_{(x,y),(l,j)}, & k > 1 \end{cases} \qquad (2)$$

依照上面的機率模型，我們可以分析出做平均 MS 在做多少次換手動作才能夠離開 ASN。以下則是比較本論文提出的方法與[4]中所訂定方法的差異：

$$H_{ASN}(l) = \frac{\sum_{x=0}^{n-1}\sum_{y=0}^{x-1}\sum_{k=1}^{\infty}\sum_{j=0}^{l-2} P_{k,(x,y),(l,j)} \cdot \left[(k-1)\cdot A_{INTRA\_ASN} + A_{INTER\_ASN}\right]}{(l+1)\cdot l/2} \quad (3)$$

其中：

A_{INTRA_ASN}：表示在一次的 Intra-ASN 換手當中，須重新做 AK Assignment 與否。其值如果爲 1 表示要做，爲 0 則否。

A_{INTER_ASN}：表示在一次的 Inter-ASN 換手當中，須重新做 AK Assignment 與否。其值如果爲 1 表示要做，爲 0 則否。

$H_{ASN}(l)$：表示一個 MS 在 *l*-階的 ASN 內平均需要執行多少次 AK Assignment 才能跨出 ASN，不包含 candidate target BSs 的 AK 配置。此時的 $H_{ASN}(l)$ 等同於 MS 換手的次數。

另外，因爲每次的handover都會關係到傳送到的封包數量，因此利用公式(3)可以將MS平均在ASN內handover的次數延伸爲傳送的封包數量。此實驗流程列出封包訊息移動時所有產生的負載(loads)，其中灰階區塊爲[4]設計的程序與本論文所提出方法的差異部份，可以說原先[4]設計的程序會比本論文多出 *T3*→*T6*，且 *T9*→*T12*。

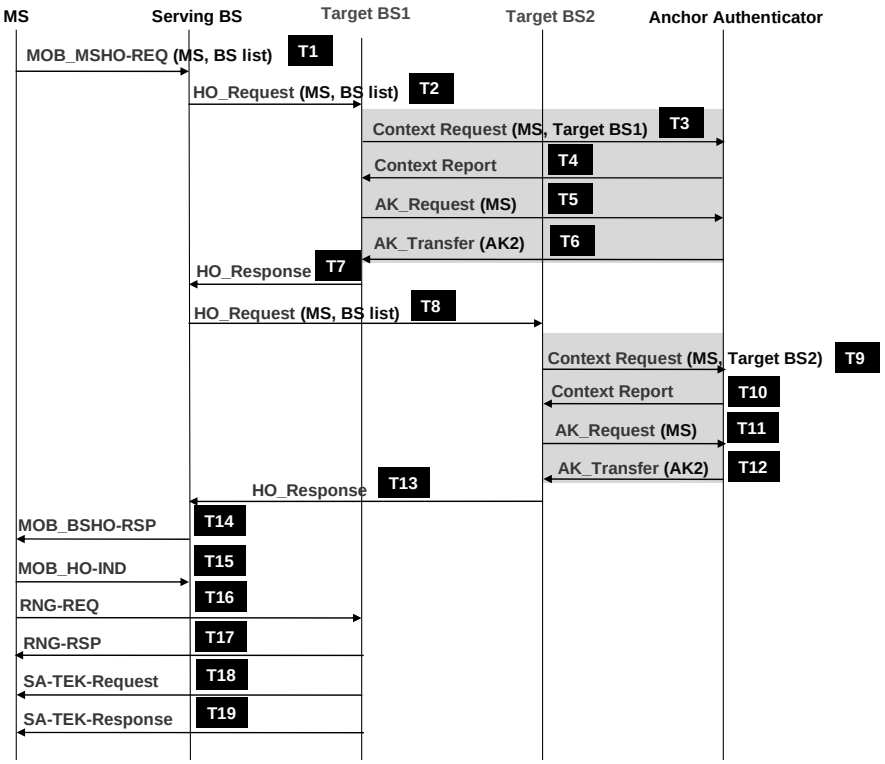


Figure 4-5 Reduced traffic loads when HO

因此可以延伸出封包傳輸所產生的traffic loads。[4]所提出的傳輸模式代入(3)即可產生下列公式(4)：

$$\mathrm{T}_{ASN}(l) = \frac{\sum_{x=0}^{n-1}\sum_{y=0}^{x-1}\sum_{k=1}^{\infty}\sum_{j=0}^{l-2} P_{k,(x,y),(l,j)} \cdot \left[(k-1) \cdot T_{\mathrm{INTRA\_ASN}} + T_{\mathrm{INTER\_ASN}} \right]}{(l+1) \cdot l/2} \qquad (4)$$

其中：

T_{INTRA_ASN}：爲一個 MS 在 ASN 內 handover 時 backhaul 端所需傳送的封包個數，包含 candidate target BSs。

T_{INTER_ASN}：爲一個 MS 在跨越 ASN 做 handover 時 backhaul 端所需傳送的封包個數，包含 candidate target BSs，Inter-ASN 的封包數量應與 Intra-ASN 相同。

$T_{ASN}(l)$：爲一個 MS 平均在 l-階的 ASN 內需做多次 handover 後跨越 ASN 所需要的封包負載量，包含 candidate target BSs。

4.2.2 NAP model

NAP之內包含一或多個ASN，因此在決定ASN架構後，如圖所示(Figure 4-6)，

將由多個ASN組合而成一個NAP。直接引用公式(3)則可求出MS可能在任何一個ASN環境底下經由handover橫跨不同的ASN。再將 ASN model的運算結果代入NAP model，才能表現出一個MS在NAP內平均要執行多少次換手動作，橫跨多少個BS才能跨出NAP。

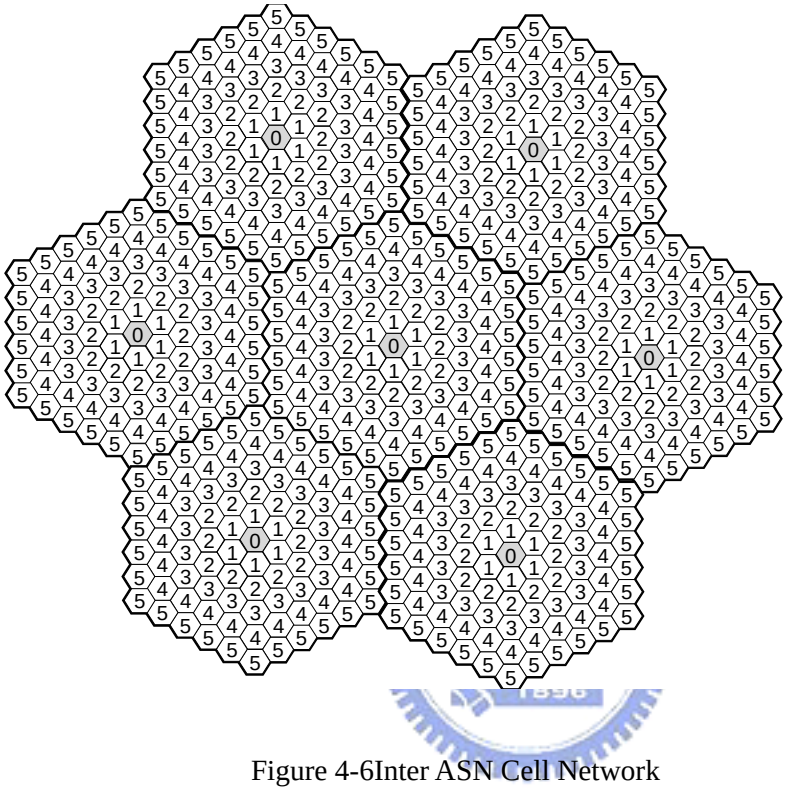


Figure 4-6Inter ASN Cell Network

當 MS 在 NAP 的涵蓋範圍下，MS 在做換手時 anchor authenticator 不需要改變，一旦跨越 NAP 後則需做 re-authentication，因此對於 AK 的 refresh 則參考公式(5)。

$$\mathrm{H}_{NAP}(l) = \frac{\sum_{x=0}^{n-1}\sum_{y=0}^{x-1}\sum_{k=1}^{\infty}\sum_{j=0}^{l-2} P_{k,(x,y),(l,j)} \cdot \left[(k-1)\cdot \mathrm{A}_{\mathrm{INTRA\_NAP}} + \mathrm{A}_{\mathrm{INTER\_NAP}} \right]}{(l+1)\cdot l/2} \qquad (5)$$

$A_{\mathrm{INTRA\_NAP}}$：預期 MS 在 Intra-NAP 範圍下隨機做 handover 須重新做 AK Assignment 與否。其值如果爲 1 表示要做，爲 0 則否。

$A_{\mathrm{INTER\_NAP}}$：MS 在 Inter-NAP 做 handover 是否須重新做 AK Assignment，其值如果爲 1 表示要做，爲 0 則否。

$\mathrm{H}_{\mathrm{NAP}}(l)$：表示一個 MS 在 l-階的 NAP 內平均需要執行多少次 AK Assignment 才能

跨出 NAP，不包含 candidate target BSs 的 AK 配置。此時的 $H_{\mathrm{NAP}}(l)$ 等同於 MS 換手的次數。

至於封包的負載，考慮 ASN model 所產生的結果代入 NAP 所產生 loads 的平均負載度爲：

$$T_{NAP}(l)=\frac{\sum_{x=0}^{n-1}\sum_{y=0}^{x-1}\sum_{k=1}^{\infty}\sum_{j=0}^{l-2}P_{k,(x,y),(l,j)}\cdot\left[(k-1)\cdot T_{\mathrm{INTRA\_NAP}}+T_{\mathrm{INTER\_NAP}}\right]}{(l+1)\cdot l/2} \tag{6}$$

T_{INTRA_NAP}：爲一個 MS 平均在每個 NAP 內透過 backhaul 端傳送封包的負載量，其值等同於 $T_{ASN}(l)$，包含 candidate target BSs 所產生的封包數量。

T_{INTER_NAP}：爲一個 MS 在跨越 NAP 時所需傳送的負載量，包含 candidate target BSs 所產生的封包數量。

$T_{NAP}(l)$：爲針對一個 MS 平均在 l-階的 NAP 內做 handover 多少次才能離開 NAP 所需要的負載量 (traffic loads)，包含 candidate target BSs 所產生的封包數量。

4.3 測試結果

4.3.1 AK assignments for an MS

首先針對 MS 在 ASN 內平均換手的次數做分析。實驗環境預設 l 爲 8 個 subarea，在 ASN 的環境下，的方式帶入公式(3)後 $H_{\mathrm{ASN}}(l)$ 結果爲：

l-subarea	Number of HOs
0	1
1	1.14
2	5.362068966
3	8.609502811
4	12.62258045
5	17.41184412
6	22.89164455
7	28.72149742

至於 NAP 的環境下，在同樣在 8-subarea 的 cluster 環境，帶入公式(5)可得 MS 在 NAP 內平均換手的次數爲 H_{NAP} ：

l-subarea	Number of HO
0	1
1	1.1988
2	14.04504756
3	38.37666001
4	81.80941986
5	151.6137228
6	255.1821088
7	395.895869

以2.3.5 節中以**MS發送MOB_MSHO-REQ給serving BS**的例子來說，MS每一次的換手動作都會造成candidate target BSs執行AK Assignment，因此，若以六個 candidate target BSs 爲例，AK Assignment的次數爲換手次數的 6 倍。

依照本論文所提出的方法，因爲MS在NAP範圍內都不需要執行AK Assignment，所以 $H_{ASN}(l)$ 保持爲 0，因此在ASN內考量candidate target BSs的情況下，本論文與原先標準所制定的方式差異如Figure 4-7所示。

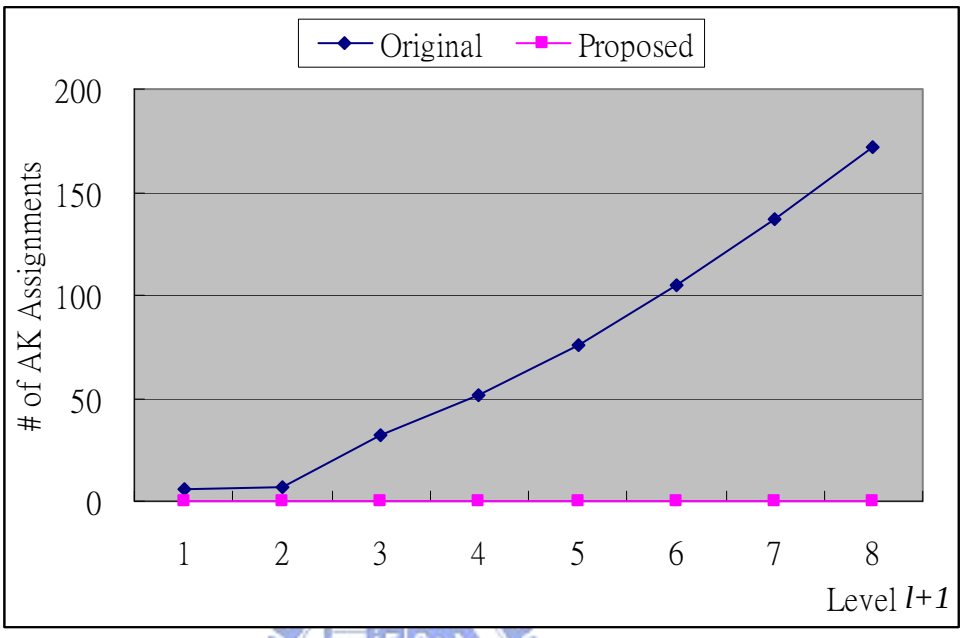


Figure 4-7 Number of AK assignments to HOs within ASN domain

至於在NAP的環境下，同樣以2.3.5 節**MS發送MOB_MSHO-REQ給serving BS**爲例子來說，AK Assignment的次數也爲 $H_{NAP}(l)$ 的 6 倍。而本論文所提出的方式在NAP內不需要執行AK Assignment，即使MS橫跨NAP須執行full authentication，也不需要執行AK Assignment。因此在同樣考量candidate target BSs的情況下一個MS在NAP內平均執行AK Assignment的次數由Figure 4-8所示。

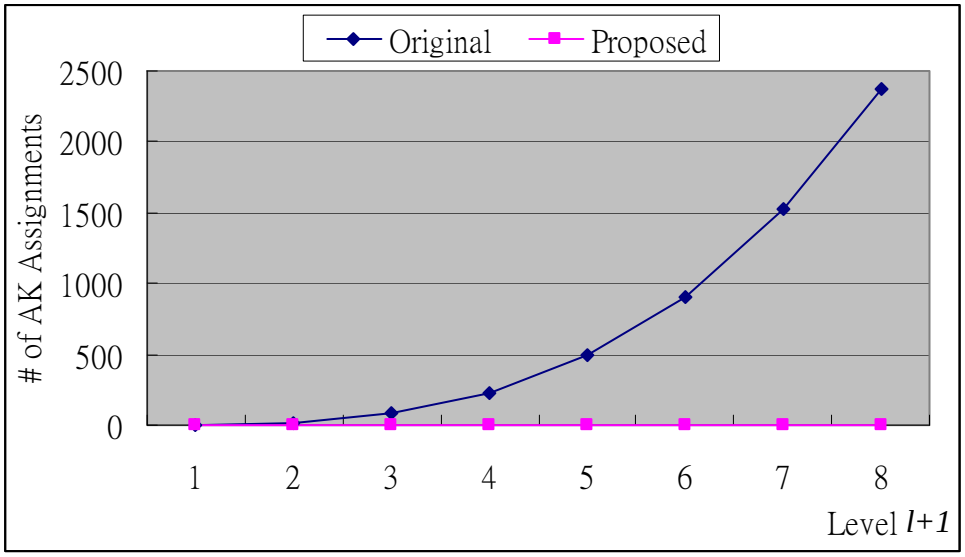


Figure 4-8 Number of AK assignments to HOs within NAP domain

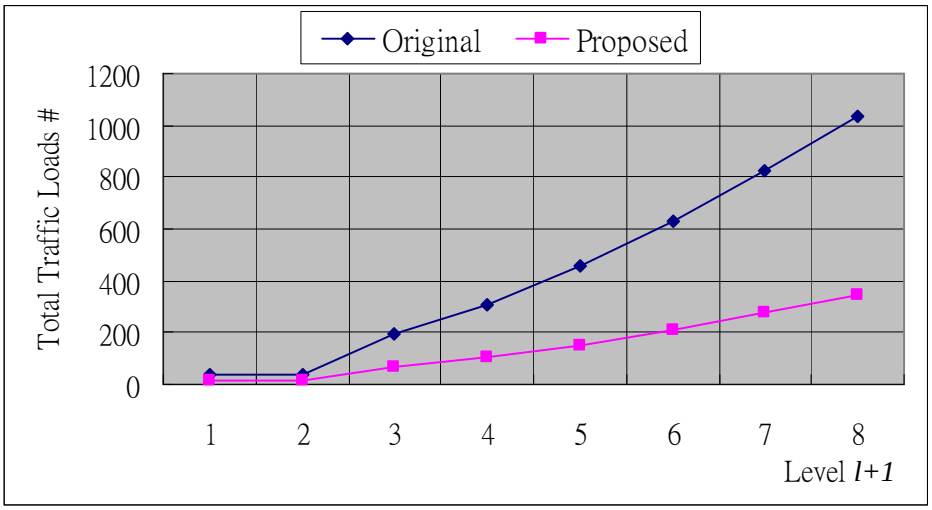
因此由上述的實驗分析可得知，不管是分析 ASN 或是 NAP，原先標準制定的方法，隨著 level 數的增加，AK Assignment 的次數也隨著增多。而本論文所提出的方式，MS 在 NAP 範圍內，因不需要執行 AK Assignment，所以 MS 在 NAP 內 AK Assignment 的次數爲 0，也因此相較於標準的制定方式，可以節省更多次的 AK Assignment，進而可以節省更多 backhaul 端的 traffic loads 和 authenticator 端的 computation loads。

4.3.2 Total Traffic Loads in an ASN/NAP caused by one MS

對於封包的負載，在**ASN**的環境下，同樣以 8 個subarea爲例，根據[4]所提出的方法，計算MS在換手時後端在處理AK refresh的網路流量。此時包括HO Request、HO Response、Context Request、Context Report、AK Request、AK Transfer。假設包含candidate target BSs，所以MS每次換手時不僅在Intra-ASN或Inter-ASN，所需的封包數量爲 36 (6 x 6 candidate BSs)。至於本論文所提出的解決方案，則因減少 AK Assignment (Context Request、Context Report、AK Request、AK Transfer)，同樣地，不僅是在Intra-ASN或Inter-ASN，MS換手時後端所需的封包數量爲 12 (2 x 6 candidate target BSs)，如下表格所示：

	Original		Proposed	
INTRA-ASN Handover	36	HO Request/Response x 6 Context Request/Report x 6 AK Request/ Transfer x 6	12	HO Request/Response x 6
INTER-ASN Handover	36	HO Request/Response x 6 Context Request/Report x 6 AK Request/ Transfer x 6	12	HO Request/Response x 6

根據表格所顯示的封包數量代入公式(4)所得到結果爲MS在ASN內平均執行換手動作時所需要的封包數量，如圖所示。其中$T_{ASN_O}(l)$表示依照[4]制訂方式，而$T_{ASN_P}(l)$則爲本論文所提出的方式。



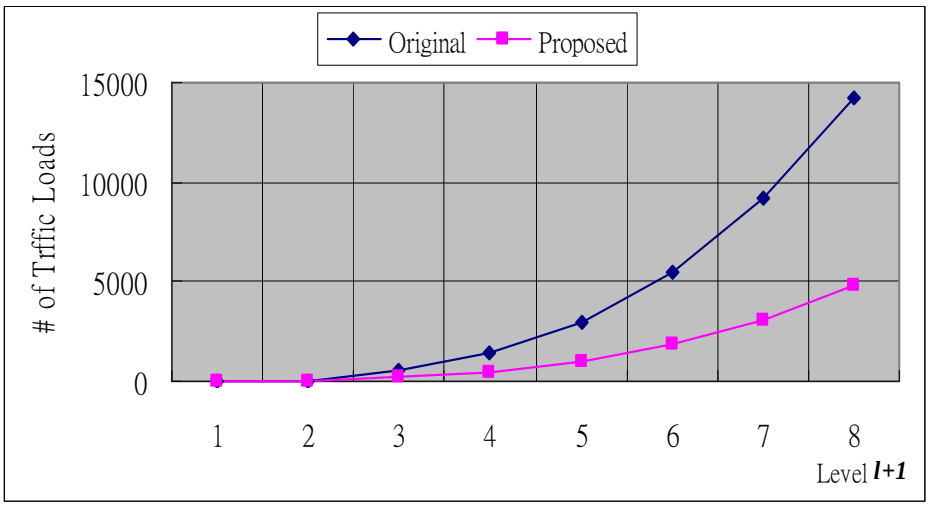
至於在NAP的情況下，依照原先[4]所定義的方式，考慮Intra-NAP及Inter-NAP的情形：在Intra-NAP的情形下，MS在NAP內平均執行換手動作時所需要的封包數量爲$T_{ASN_O}(l)$。至於在Inter-NAP的情形下，MS在橫跨不同的NAP時，AK的獲得必需透過full-authentication才能得到，而執行full authentication時負責處理認證訊息的authenticator則爲不同NAP底下的anchor authenticator，因此只需考慮原先服務MS的NAP即可。所以MS換手時僅考慮發出的HO Request與HO Response， $T_{ASN_O}(l)$會只扣除掉AK Assignment的封包數量，保留HO Request/Response，得到結果爲$T_{ASN_O}(l) - 24$。至於本論文所提出的方式，同樣的考慮Intra-NAP與Inter-NAP的情形：在Intra-NAP

的情形下，MS在NAP內執行換手動作時所需要的封包數量爲$T_{ASN_P}(l)$。至於Inter-NAP則同樣執行full authentication，因此僅需考慮 HO Reques/Response即可。因此在Inter-NAP時所需的平均封包數量爲 $T_{ASN\_P}(l)$。因此帶入公式(6)的結果爲：

	Original		**Proposed**	
INTRA-NAP Handover	$T_{ASN\_O}(l)$		$T_{ASN\_P}(l)$	
INTER-NAP Handover	$T_{ASN\_O}(l)$ -24	HO Request/Response x 6	$T_{ASN\_P}(l)$ -12 +12	HO Request/Response x 6

l-subarea	T_{NAP_O} (Original)	T_{NAP_P} (Proposed)
0	12	12
1	28.7568	14.3856
2	481.6217112	168.5405706
3	1357.559763	460.5199217
4	2921.139113	981.7130364
5	5434.094914	1819.364698
6	9162.568073	3062.18531
7	14228.31941	4750.750479

將結果由圖表顯示如下：



由圖表可以得知幾點事項：

1) 原先[4]所描述的方法，無論ASN或是NAP的環境下，隨著level數的增加，Traffic Loads 也隨之增加。

2) 本論文所提出的方法，因不需要執行 AK Assignment，因此隨著 level 數增加，可以節省的 Traffic Loads 也隨之增加。

4.3.3 Loads of Anchor Authenticator

本論文所提出的方法，是採用分散式方法(distributed)，由 serving BS 傳送 AK Context 給 candidate target BSs，來取代中央控管(centralized)的方式，由 anchor authenticator 傳送 AK 給 candidate target BSs。因此每當 MS 在 handover 時採用分散式的方式取得 AK 時，anchor authenticator 節省 AK Assignment 所需的封包(Context Request、Context Report、AK Request、AK Transfer，Context Request)。亦即多台 MS 同時 handover 的數量越多，anchor authenticator 節省的負載量越多。因此在 NAP 的範圍內：

anchor authenticator 可以節省計算 AK 的計算量為：$H_{NAP}(l) * N_{MS} * 6 * c$

$H_{NAP}(l)$：為 MS 在 NAP 內平均換手的次數；

N_{MS}：為單一時間內，anchor authenticator 同時收到 MS 提出計算 AK 的需求；

6：表示 MS 在執行換手動作時，candidate target BS 也跟著提出計算 AK 的需求；

c：表示 anchor authenticator 在計算 AK 時所花費的時間。

第 5 章
結論與未來工作

綜合考量 AK 重新取得的次數與網路傳輸的負載度，本論文所提出的方法在效能上明顯比原先的流程較好。此外不僅是在 ASN 或是在 NAP 的環境下，隨著 *l* 的階層數越高，降低網路負載的效果較爲明顯，減少 anchor authenticator 計算 AK 所花費的時間也越明顯。

另外，本論文在提出方論點時，是按照 WiMAX 的架構及原先設計的精神，在兼顧安全性的考量下所設計。所以在討論結論與未來工作之前，首先了解本論文所以提出的論述與考慮方向，經由哪些考量點，再來評估往後的發展。因此本論文先針對：1) 修改 AK 公式的各種可行性分析。2) AK Context 在 handover 過程時的傳送路徑，在此提出分析過程。

針對修改AK的產生公式，根據[3]所提出關於AK的公式：

AK=Dot16KDF(PMK, SS MAC Address | BSID | “AK”, 160)

在欲修改BSID爲之前，首先分析目前WiMAX網路上有哪些ID可以選擇？參照[5]所提供的ID (表格 A-6)，除了有原先的BS ID之外，還包含Operator ID (NAP ID)、NSP ID、Authenticator ID。我們針對各個ID做評估分析：

1) **NSP ID**：

優點：[5]中所描述，NSP ID爲全域變數，因此NSP ID爲整個WiMAX中均可以獲得。所以MS在initial network entry時可以透過SBC-REQ向BS提出，BS即可透過SBC-RSP給予回應。MS不需爲獲得NSP ID而增加額外的負擔。

缺點：若將 NSP ID 帶入公式，則 AK 可使用的涵蓋範圍擴大到 NSP 所對應到的 NAP(1 或多個 NAP)，除非跨越不同的 NSP，否則 AK 在這 NSP 底下的多個 NAP 範圍內不會改變。這幾乎否決 key 存在的意義。在安全性的考量下，理應 key 的範

圍越小越好，知道的人也越少越好。

2) **Authenticator ID：**

優點：Authenticator ID 的涵蓋範圍與 NSP ID 比較下相對較小。

缺點：如(表格 A-6)所示，Authenticator ID爲在Intra-ASN範圍內傳送，所以MS並無法獲得Authenticator ID。此外爲了讓MS獲得此ID則必須增加額外的流程。另外，當MS在做handover時，若將AK產生公式的參數由原先的target BS ID改爲target Authenticator ID，對於先前描述AK的產生是由anchor authenticator所產生，anchor authenticator 裡應不知道target Authenticator ID (anchor authenticator不曉得MS handover的target BS是屬於哪一個authentication domain)，若是選擇anchor Authenticator ID，則又與原先 802.16e訂定MS再換手時須使用target BS ID來產生AK的精神相違背。

3) **NAP ID：**

優點：

a) MS 透過 DL-MAP 可以獲得 NAP ID(BS ID 的前 24bits)，不需增加額外流程。

b) NAP 的涵蓋範圍比 NSP 小。

c) MS handover過程中，在mobility domain的範圍內(包含一個或多個authentication domain)，一般爲NAP，AK統一由anchor authenticator所產生。因此認爲使用NAP ID比較符合[4]的設計架構。

d) NAP ID 帶入公式後，MS 在 handover 過程中，只要是在 NAP(mobility domain)的涵蓋範圍下，在生命週期內(lifetime)不需重新產生 AK，可減少後端網路的負擔。

缺點：

AK 產生的涵蓋範圍由原先的 MS 與 BS 之間擴大爲 MS 與 NAP 之間。在 NAP 涵蓋範圍下 MS 與任何 BS 相連接均使用同一把 AK。爲了安全性的考量，必須儘量讓越少的 BS 知道 MS 的 AK Context。

綜合前面三種 ID 的評估後，本論文因此選擇使用 NAP ID 爲最後決定，至於 NAP 所產生的缺點，則藉由減少 AK Context 的分布，補強使用 NAP ID 所帶來的缺點。

既然選擇NAP ID爲本論文修改公式的參數後，在Mobility domain (通常爲NAP)底下的AK爲同一把，接下來的討論爲AK Context應該由誰傳送以及誰可收到AK Context。[4]描述在Mobility domain底下由anchor authenticator依據target BS提出AK Request 和 Context Request傳送AK Context給target BS；爲了節省 AK Request與Context Request的傳輸訊息所花費的時間與縮短anchor authenticator與target BS之間的距離，本論文利用AK在NAP底下爲同一把的特性，選擇serving BS在通知candidate target BSs有開始啓動handover的同時，挾帶著AK Context資料給candidate target BSs。藉此只讓serving BS週遭的candidate target BSs擁有MS的AK Context，以減少AK的分布，來強化其安全性。另外，也因爲serving BS取代anchor authenticator來傳送AK Context，原先anchor authenticator與candidate target BSs之間的距離縮短爲serving BS與candidate target BSs之間的距離，減少因距離而產生的延遲(參照2.3.2)。

既然已選擇由serving BS取代anchor authenticator傳送AK給target BS，該透過什麼時間點與什麼訊息傳送，本論文考慮2.3.5所描述的三個時間點，以及目前後端訊息傳送的各種封包訊息，發現透過HO Request封包夾帶AK Context，若選擇已知的HO Request通知candidate target BSs並不會增加額外的機制，而且可以讓target BS事先獲的MS的AK Context。因此決定在serving BS欲發出HO Request的訊息給candidate target BSs的時間點同時夾帶AK Context。

在原先 WiMAX Forum 的設計架構下，MS 在 handover 的過程中，後端(backhaul)網路須負責爲 MS 處理相當多的流程(包含 authentication、path registration、MIP 等等)，也因此大大增加了 handover 的延長時間與網路負擔，因此簡化後端流程爲相當重要的課題。

透過以上的分析與設計，本論文在經過實驗與分析後，實際加速了 MS 在 handover 的流程，也降低了網路後端的負擔，更減少 anchor authenticator 的運算負

載。

關於未來工作的部分，WiMAX Forum持續在針對[4][5]做修正與改進，[2]也持續在爲認證程序構思簡化方法，以求達到seamless的效果。


E
S
A
1896

Reference

[1] B. Aboba, et al., “Extensible Authentication Protocol (EAP)”, RFC 3748, June 2004.

[2] IEEE Standard for Local and metropolitan area networks Part 16: 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 and Corrigendum 1, IEEE Std 802.16e-2005 and IEEE Std 802.16-2004 / Cor 1-2005, 2006.

[3] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004, 2004.

[4] WiMAX Forum NWG Stage 2, release 1 V&V draft, August 8, 2006.

[5] WiMAX Forum NWG Stage 3, release 1 V&V draft, August 8, 2006.

[6] Simon Blake-Wilson “TLS Inner Application Extension(TLS/IA)”, TLS Working Group, October 2004

[7] I. F. Akyildiz,Y.-B. Lin,W.-R. Lai, and R.-J. Chen, "A new random walk model for PCS networks," IEEE J. Select. Areas Commun., vol. 18, pp. 1254–1260, 2000.

[8] G. Xue, “An Improved Random Walk Model for PCS Networks,” IEEE Transactions on Communications, vol. 50, no. 8, pp. 1224-1226, August 2002.

[9] David Johnston and Hassan Yaghoobi, “Peering Into the WiMAX Spec,” CommsDesign, www.commsdesign.com, 21 Jan, 2004.

附錄A

表格 A-1 HO Request transmitted within ASN

IE	Description	M/O
HO Type	Describes type of the HO (FBSS, MDHO, HHO)	M
MS Info	Contains HO-related MS context in the nested IEs	M
>MS ID	6 octet MS ID (MAC Address)	M
>Anchor GW ID	Identifies the Anchor ASN GW	M
>Authenticator GW ID	Identifies the Authenticator GW	M
>R3MM Context	R3MM related Context Info	O
>SF Info (one or more)	Each IE of the list contains context of a particular SF.	M
>>SFID	SFID associated with the Service Flow	M
>>CID	CID associated with the Service Flow in the Serving BS	M
>>SAID	SAID associated with the Service Flow	M
>>TEK Context	TEK context might be included if there is a desire to share TEKs between the Serving and Target BS upon HO.	O
>>Packet Classification Rule (one or more)	Each IE in the list contains IEEE 802.16e Packet Classification Rule	O
>>>Classifier Rule Priority	IEEE 802.16e Classifier Rule Priority	O
>>>Classifiers	Set of IEEE 802.16e Classifiers associated with the Classifier Rule	O
>>QoS Info	QoS Parameters associated with the Service Flow	O
>>>QoS Parameters	IEEE 802.16 QoS Parameters	O
Serving BS Info	Contains Serving BS context in the nested IEs.	M
>BS ID	Serving BS ID	M
>Round Trip Delay	Round Trip Delay (RTD) between the MS and the Serving BS	O

>DL PHY Quality Info	Downlink PHY Quality between the MS and the Serving BS	O
>UL PHY Quality Info	Uplink PHY Quality between the MS and the Serving BS	O
Target BS Info (one or more)	Each IE in the list contains Target BS context in the nested IEs.	M
>BS ID	Target BS ID	M
>Data Path Establishment Option	A flag indicating whether or not Data Path should be established before responding to the HO Request.	O
>Relative Delay	Indicates the delay of neighbor DL signals relative to the serving BS, as measured by the MS for the particular BS.	O
>DL PHY Quality Info	Downlink PHY Quality between the MS and the Serving BS	O
>UL PHY Quality Info	Uplink PHY Quality between the MS and the Serving BS	O

表格 A-2 Context Request from Target BS

IE	Description	M/O
HO Type	Describes type of the HO (FBSS, MDHO, HHO)	M
MS Info	Contains HO-related MS context in the nested IEs.	M
>MS ID	6 octet MS ID (MAC Address)	M
Serving BS Info	Contains relevant Serving BS context in the nested IEs.	O
>BS ID	Serving BS ID	O
Target BS Info	Contains relevant Target BS context in the nested IEs.	M
>BS ID	Target BS ID	M

表格 A-3 Context Report to Target BS

IE	Description	M/O
MS Info	Contains HO-related MS context in the nested IEs.	M
>MS ID	6 octet MS ID (MAC Address)	M

>Service Authorization	Indicates whether or not the service is authorized, if not specifies reason.	O
>Authenticator AK Context	Contains AK Context in the nested IEs	M
>>AK	160-bit AK	M
>>AK ID	64-bit AK ID	M
>>AK Lifetime	16-bit AK Lifetime (in seconds)	M
>>AK SN	4-bit AK SN	M
>>PMK SN	4-bit PMK SN	M

表格 A-4 HO Response

IE	Description	M/O
HO Type	Describes type of the HO (FBSS, MDHO, HHO)	M
Result Code	The result of the Request	M
MS Info	Contains HO-related MS context in the nested IEs.	M
>MS ID	6 octet MS ID (MAC Address)	M
Serving BS Info	Contains relevant Serving BS context in the nested IEs.	M
>BS ID	Serving BS ID	M
Target BS Info (one or more)	Contains relevant Target BS context in the nested IEs.	M
>BS ID	Target BS ID	M
>Temporary BS ID	Temporary ID assigned to the target BS	O
>HO ID	ID assigned for use in initial ranging to the target BS once this BS is selected as the target BS	O
>Service Level Prediction	Service Level Prediction code.	O
>Preamble Index / Subchannel Index	Preamble Index / Sub-channel Index code	O
>HO Process Optimization	HO Process Optimization code	O
>SF Info (one or more)	Each IE of the list contains context of a particular SF.	M

>>SFID	SFID associated with the Service Flow	M
>>CID	CID replacement	M
>>SAID	SAID replacement	M
>>SDU Info	First Buffered/Multicast SDU context for Data Integrity. Relevant only for DL U-Cast Service Flows.	O
>>>SDU SN	Sequence Number of the First Buffered/Multicast SDU context for Data Integrity. Relevant only for DL U-Cast SF.	O

表格 A-5 AK Context

Parameter	Size(bits)	Usage
AK	160	The authorization key
AKID	64	AKID = Dot16KDF(AK, AK SN|SS MAC Address|BSID|"AK", 64). The AK_SN in the Dot16KDF function is an 8-bit number which consists of leading 4 zero bits and appending 4-bit AK_SN in MSB first order.
AK Sequence Number	4	Sequence number of AK. If AK = f (PMK and PMK2), then AK SN = PMK SN + PMK2 SN If AK = f (PMK), then AK SN = PMK SN
AK Lifetime		This is the time this key is valid; it is calculated AK lifetime =MIN(PMK lifetime, PMK2 lifetime) - when this expires, re -authentication is needed.
PMK Sequence Number	4	The sequence number of the PMK that this AK is derived from
PMK2 Sequence umber	4	The sequence number of the PMK2 that this AK is derived from. In Single-EAP, it shall always set to zero
CMAC_KEY_U	160/128	The key which is used for signing UL management messages
CMAC_PN_U	32	Used to avoid UL replay attack on the management connection–before this will expire (for example, when

		CMAC_PN_D value bigger than 2_{32} – 10, 000) re-authentication is needed. The initial value of CMAC_PN_U is zero and the value of CMAC_PN_U is reset to zero whenever CMAC_KEY_COUNT is increased.
CMAC_KEY_D	160/128	The key which is used for signing DL management messages
CMAC_PN_D	32	Used to avoid DL reply attack on the management connection –before this will expire (for example, when CMAC_PN_D value bigger than 2_{32} – 10, 000) re-authentication is needed. The initial value of CMAC_PN_D is zero and the value of CMAC_PN_D is reset to zero whenever CMAC_KEY_COUNT is increased.
KEK	160	Used to encrypt transport keys from the BS to the SS
EIK	160	EAP Integrity Key for authenticating Authenticated EAP message.
CMAC_KEY_COUNT	16	Value of the Entry Counter that is used to guarantee freshness of computed CMAC_KEY_* with every entry and provide replay protection. Upon initial network entry, count is reset to 0 in the MS and Serving BS, and to 1 in the Authenticator.

表格 A-6 List of Identifier

Identifier	Type	Size	Scope(area of validity)
BS ID	binary	48 bits	Global
Operator ID	binary	24 bits	Global
NSP ID	binary	24 bits/32 char string	Global

Authenticator ID	binary	4 octets/16 octets	NAP/NSP

表格 A-7 Proposed HO Request transmitted within ASN

IE	Description	M/O
HO Type	Describes type of the HO (FBSS, MDHO, HHO)	M
MS Info	Contains HO-related MS context in the nested IEs	M
>MS ID	6 octet MS ID (MAC Address)	M
>Anchor GW ID	Identifies the Anchor ASN GW	M
>Authenticator GW ID	Identifies the Authenticator GW	M
>R3MM Context	R3MM related Context Info	O
>SF Info (one or more)	Each IE of the list contains context of a particular SF.	M
>>SFID	SFID associated with the Service Flow	M
>>CID	CID associated with the Service Flow in the Serving BS	M
>>SAID	SAID associated with the Service Flow	M
>>TEK Context	TEK context might be included if there is a desire to share TEKs between the Serving and Target BS upon HO.	O
>>Packet Classification Rule (one or more)	Each IE in the list contains IEEE 802.16e Packet Classification Rule	O
>>>Classifier Rule Priority	IEEE 802.16e Classifier Rule Priority	O
>>>Classifiers	Set of IEEE 802.16e Classifiers associated with the Classifier Rule	O
>>QoS Info	QoS Parameters associated with the Service Flow	O
>>>QoS Parameters	IEEE 802.16 QoS Parameters	O
Serving BS Info	Contains Serving BS context in the nested IEs.	M
>BS ID	Serving BS ID	M

>Round Trip Delay	Round Trip Delay (RTD) between the MS and the Serving BS	O
>DL PHY Quality Info	Downlink PHY Quality between the MS and the Serving BS	O
>UL PHY Quality Info	Uplink PHY Quality between the MS and the Serving BS	O
Target BS Info (one or more)	Each IE in the list contains Target BS context in the nested IEs.	M
>BS ID	Target BS ID	M
>Data Path Establishment Option	A flag indicating whether or not Data Path should be established before responding to the HO Request.	O
>Relative Delay	Indicates the delay of neighbor DL signals relative to the serving BS, as measured by the MS for the particular BS.	O
>DL PHY Quality Info	Downlink PHY Quality between the MS and the Serving BS	O
>UL PHY Quality Info	Uplink PHY Quality between the MS and the Serving BS	O
AK Context	**Contains AK Context in the nested IEs**	**M**
>AK ID	**64-bit AK ID**	M
>AK Lifetime	**16-bit AK Lifetime (in seconds)**	M
>AK SN	**4-bit AK SN**	M
>PMK SN	**4-bit PMK SN**	M

表格 A-8 HO Request transmitted across ASN

IE	Description	M/O
HO Type	Describes type of the HO (FBSS, MDHO, HHO)	M
MS Info	Contains HO-related MS context in the nested IEs	M
>MS ID	6 octet MS ID (MAC Address)	M
>Anchor ASN GW ID	Identifies the node that hosts the Anchor DP Function in the Anchor ASN. If it is not included, it means that the originator of HO Request hosts the Anchor DP Function for the MS.	O

>Authenticator ID	Identifies the node that hosts Authenticator and Key Distributor Function in the Authenticator ASN. If it is not included, it means that the originator HO Request hosts the Authenticator and Key Distributor Function for the MS.	O
>R3MM Context	R3MM related Context Info	O
>SBC Context	SBC related Context Info	O
>REG Context	REG related Context Info	O
>PKM Context	PKM related Context Info	O
>AK Context	AK related Context Info. May be included if the Serving ASN retrieves the AK Context from the Authenticator ASN	O
>Data Path Info	DL (Anchor to Target) Data Path Info for per-BS or per-MS granularity tunnel. It may be optionally included in the function collocation case and if per-BS or per-MS granularity tunnel is supported between the Anchor and Target ASNs.	O
>SF Info (one or more)	Each IE of the list contains context of a particular SF.	M
>>SFID	SFID associated with the Service Flow	M
>>CID	CID associated with the Service Flow in the Serving BS	M
>>SAID	SAID associated with the Service Flow	M
>>Data Path Info	DL (Anchor to Target) Data Path Info for per-flow granularity tunnel. It may be optionally included in the function collocation case and if per-SF granularity tunnel is supported between the Anchor and Target ASNs.	O
>>TEK Context	TEK context might be included if there is a desire to share TEKs between the Serving and Target BS upon HO.	O
>>Packet Classification Rule (one or more)	Each IE in the list contains IEEE 802.16e Packet Classification Rule	O
>>>Classifier Rule Priority	IEEE 802.16e Classifier Rule Priority	O

>>>Classifiers	Set of IEEE 802.16e Classifiers associated with the Classifier Rule	O
>>QoS Info	QoS Parameters associated with the Service Flow	M
>>>QoS Parameters	IEEE 802.16 QoS Parameters	M
Serving BS Info	Contains Serving BS context in the nested IEs.	M
>BS ID	Serving BS ID	M
>Round Trip Delay	Round Trip Delay (RTD) between the MS and the Serving BS	O
>DL PHY Quality Info	Downlink PHY Quality between the MS and the Serving BS	O
>UL PHY Quality Info	Uplink PHY Quality between the MS and the Serving BS	O
Target BS Info (one or more)	Each IE in the list contains Target BS context in the nested IEs.	M
>BS ID	Target BS ID	M
>Data Path Establishment Option	A flag indicating whether or not the Target ASN should instigate Data Path (Pre -)Registration.	O
>Relative Delay	Indicates the delay of neighbor DL signals relative to the serving BS, as measured by the MS for the particular BS.	O
>DL PHY Quality Info	Downlink PHY Quality between the MS and the Serving BS	O
>UL PHY Quality Info	Uplink PHY Quality between the MS and the Serving BS	O