WLAN 與 cellular 整合網路中支援快速換手的用戶識別模組認證機制

A Novel SIM-based Authentication Mechanism for Supporting Fast Handover in WLAN/Cellular Integrated Networks

黃郁仁
工研院電通所
yrhuang@itri.org.tw

楊人順
工研院電通所
jsyang@itri.org.tw

曾建超
國立交通大學資訊工程學系
cctseng@csie.nctu.edu.tw

摘要

在本論文中我們針對無線區域網路(Wireless LAN, WLAN)**環境，提出跨存取點**(Access Point, AP)**快速換手**(inter-AP fast handover)**的快速認證方案**(fast authentication scheme)**，以滿足多媒體傳輸之服務品質要求。此方案係以** Subscriber Identity Module **為基礎**(SIM-based)**的認證程序**(authentication procedure)**結合訊息完整性檢查**(message integrity check)**、資料隱密**(data privacy)**與先期認證**(pre-authentication)**等技術，提出更安全的新雙向認證**(Novel full authentication)**機制和跨存取點的快速換手機制等兩項貢獻。其中前者可預防假造的網路設備竊取使用者的機密資料(包括金鑰)，而後者包含金鑰先期投遞**(Key pre-distribution)**機制和非同步於** MN **換手動作的再認證機制，金鑰先期投遞可免去行動台**(Mobile Node, MN)**在換手時與** network **的再認證動作，非同步於** MN **換手動作的再認證機制可加強金鑰的安全性。如此一來，除了可以加強安全性和節省** inter-AP handover **所花費的時間外，同時也可以讓** WLAN **與行動電話網路**(cellular network)**採用同樣的認證機制，為後第三代** (Beyond 3G, B3G) WLAN/cellular network **系統間(跨階層)漫遊的** fast handover **鋪路。**

關鍵詞：以 SIM **為基礎之認證，跨存取點快速換手，公眾區域網路之保全，後第三代行動通訊**

Abstract

In this paper, we propose a fast authentication scheme for inter-AP fast handover in WLAN. This scheme is designed based on SIM-based authentication procedure and relies on message integrity check, data privacy and pre-authentication four techniques together in order to eliminate re-authentication requirement during handover. The contributions include a novel full authentication mechanism and an Inter-AP fast handover mechanism. With the first mechanism, we can avoid the stolen of user's privacy data (including the encryption key) by a fake AP. With the second mechanism, we cannot only shorten the inter-AP handover delay but also provide an identical authentication mechanism for both WLAN and cellular network. The identical authentication scheme makes the possibility of further inter-system (inter-tier) fast handover in B3G (Beyond Third Generation) Mobile Communication systems.

Keywords：SIM-based authentication，inter-AP fast handover，public WLAN security，B3G Mobile Communication

一、簡介

整合 WLAN **與** cellular network **的第一步是整合其認證的機制，目前第二代通訊系統中** GSM/GPRS **的認證機制便是建立在以** SIM **卡為標準使用者識別方式，**SIM **卡的一項相當大的優點便是提供平台的可攜性**(device portable)**，讓認證的依據由手機轉移到** SIM **卡身上，方便不受限制的移轉性的確幫助** GSM/GPRS **的用戶可以輕鬆自由的更換手機。現在** WLAN **如果能同樣以** SIM **做為認證的模組，則將統一** WLAN **與** cellular network **的認證依據，除了有助於安全機制的完善，也可統一收費系統於一體，再加上免除使用者須再申辦的麻煩程序，對未來** B3G **的發展有極**

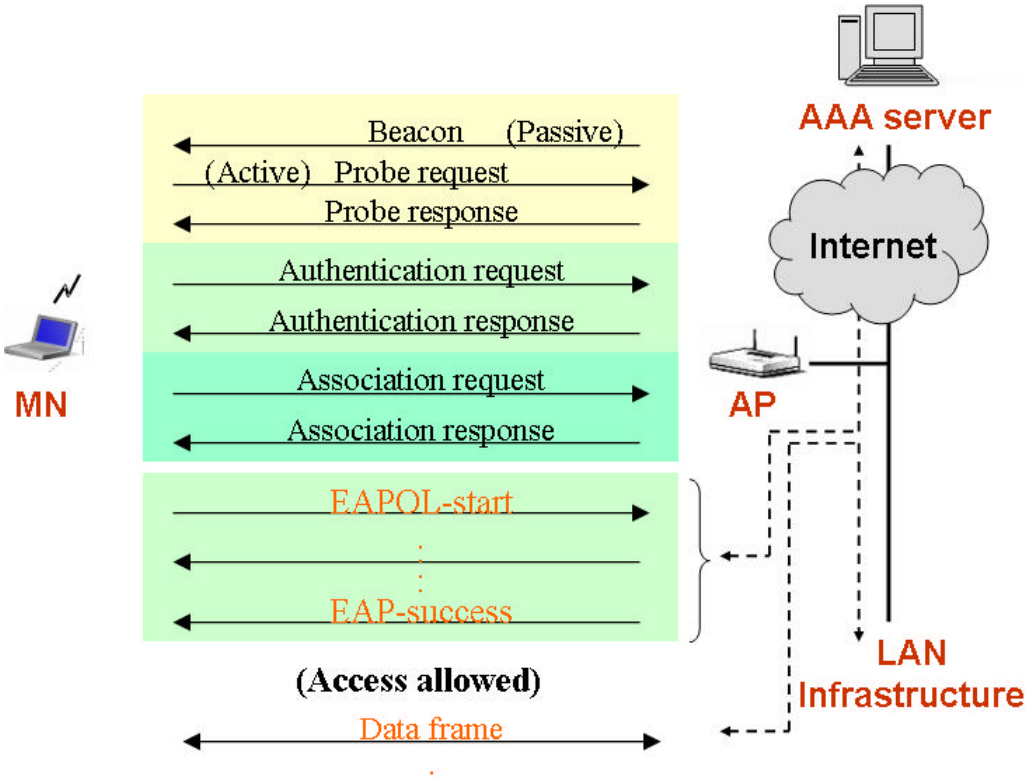

圖 1-1 IEEE 802.1x port-based network access control

為重要的幫助。

MN 在 WLAN 在不同的 AP 環境下換手(handover)一般而言會有三項生延遲，分別是 probe delay、authentication delay、re-association delay [1]，這三者都是屬於 IEEE 802.11 標準中 MN 要和 WLAN 結合(association)時所規範的步驟。然而，因其 authentication 是以 WEP 為基礎，有著安全上的嚴重的缺陷。所以目前多以 IEEE 802.1x port-based access control 的規範(如圖 1-1)來彌補 IEEE 802.11 認證方面的不足，IEEE 802.1x 的認證程序是置於 IEEE 802.11 association 建立完之後，也是整個 handover 過程中可能最花時間的階段，因為大型 public WLAN 系統，其負責認證的 Authentication, Authorization and Accounting 伺服器(簡稱 AAA server)往往置於遠端機房當中，如果 handover 時還須要做與 AAA server 做再認證的動作時必定會造成不少的延誤。因此在本論文中，我們針對 MN 的 inter-AP handover，希望能夠在消除 IEEE 802.1x 再認證延遲的同時，又能保有整體的安全性，祈能達成 fast handover 的目標。

本論文針對 WLAN 的 inter-AP fast handover 提出快速認證方案(fast authentication scheme)，以滿足多媒體傳輸之服務品質要求。此方案結合訊息完整性檢查(message integrity check)、資料隱密(data privacy)與先期認證(pre-authentication)等技術，提出更安全的新雙向認證(full authentication)機制和跨存取點的快速換手機制。其中前者可預防假造的網路設備竊取使用者的機密資料(包括金鑰)，而後者包含金鑰先期投遞(Key pre-distribution)機制和非同步於 MN 換手動作的再認證機制，金鑰先期投遞可免去 MN 在換手時與 network 的再認證動作，非同步於 MN 換手動作的再認證機制可加強金鑰的安全性。因此，一開始 MN 連接上 WLAN，經過改良之 IEEE 802.1x新雙向認證機制後，以取得的金鑰對所有訊息加以加密及訊息認證 MIC (message integrity code)的保護，不同 MN 使用不同金鑰即可建立與 AP 間的專屬安全通道，尚未換手前利用 Key pre-distribution 機制由 AAA server 將該金鑰預先投遞到臨近的 AP，一旦當 MN 需要換手時，即可以相同金鑰與臨近新 AP 繼續維持該安全通道的存在，由於 Hacker 無法取得金鑰，所以他送出的封包將無法被 AP 所辨識而遭丟棄，此為快速換手機制。此機制讓 MN 於 AP 間換手時跳過 IEEE 802.1x 再認證的動作，將可節省許多的時間又能繼續維持其安全性。至於為了進一步維持金鑰的安全，我們利用定期更新的再認證機制去定期更新金鑰，同時我們將它移到其他時間以在不影響資料的傳送，再認證的動作非同步於 MN 的換手動作且的情況下於背景執行，讓再認證的動作對使用者資料傳輸的影響減到最小。

文章的其餘部分規劃如下：第二節說明現

有 SIM-based 認證的相關協定，並且說明我們會用到哪些協定；第三節描述我們提出的 Inter-AP fast handover 的快速認證機制，其中會說明此機制的有效性和安全性；最後一節是結論。

二、SIM-based 認證的相關協定

以 SIM-based 為認證技術的基本架構裡，認證封包從 MN 為起點到最後的 cellular network 上的認證中心(AuC; Authentication Center)，一路上必須經過包括 WLAN、Internet 與 cellular network 三個網路主體。這些網路利用數種通訊協定將數個不同角色的節點串聯在一起，圖 1-1 的 protocol stack 說明本論文中參與 SIM-based 認證所須要的節點與相關協定。

在 2-1 圖中，我們特別針對 EAP (Extensible Authentication Protocol)、IEEE 802.1x 的 EPAOW (EAP over Wireless LAN)與 AAA server 上使用的 Diameter protocol 簡介其功能。

2.1 EAP protocol

EAP protocol 是 IETF RFC 2284 文件裡所提出的，原本是用來支援 PPP (Point to Point Protocol)於認證階段(authenticate phase)時所採用的其中一種認證方法，由於 EAP 本身的可擴充性設計，因此 protocol 本身並不限制使用何種認證的機制與演算法，僅透過 EAP 做雙向交握時再來決定雙方採用何種認證機制，例如 MD5-challenge，OTP (One Time Password)或 token card 等等，這裡我們將會利用 EAP 並採用 SIM-based 的認證，既是由 EAP 封包來攜帶 SIM-based 認識所須要的所有資訊。

2.2 EAPOL/EPAOW protocol

IEEE 802.1x 是一種 port-based network access control 技術，其中的 EAPOL/EPAOW 是將 EAP protocol 直接載於 LAN 或 WLAN MAC layer 之上的封包格式與協定，EAPOL 僅簡單定出五種 packet type:

(1) EAP-packet

(2) EAPOL-Start

(3) EAPOL-Logoff

(4)EAPOL-Key

(5) EAPOL-Encapsulated-ASF-Alert

其中第一項的 EAP-packet 主要就是用來承載 EAP protocol，第二至第五項分別是 EAPOL 認證過程中所使用的四種封包。由於 IEEE 802.1x 裡分成的 Supplicant、Authenticator 與 Authentication Server 三個角色，在本論文中將分別由 MN，AP (Access Point)與 AAA server 來扮演。因此我們參考 IEEE 802.1x 的認證方式，由 AP 負責對 MN 所發出的 MAC 封包做管制，只有通過認證的 MN 所發出的封包才能通過 AP 進入網路，其他尚未通過認證的 MN 必需先透過 EAP 經由 AP 向 AAA server 進行認證程序。

2.3 RADIUS (Remote Access Dial In User Service)與 Diameter 協定

RADIUS [12]與 Diameter [13]均為認證協定，都是作為 IEEE 802.1x 中 authenticator 與 authentication server 之間的通訊協定。

RADIUS 是目前市面上較為普遍支援的一套認證協定，在許多的 Windows 或 Unix 系列的伺服器中，多有 RADIUS 認證模組可供

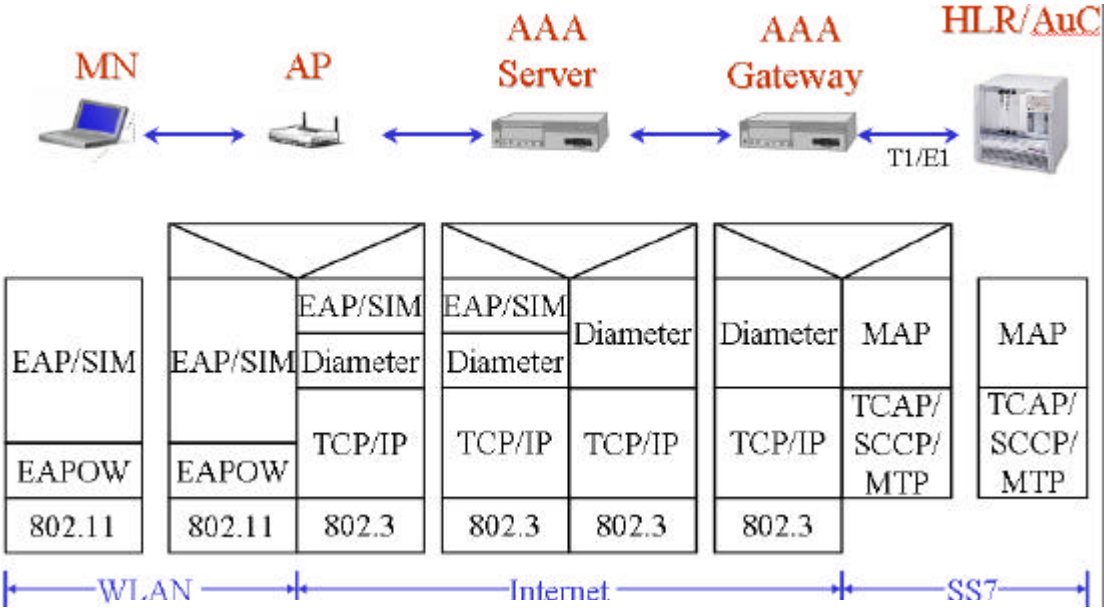

圖 2-1 SIM-based authentication protocol stack

選擇。RADIUS 早期的應用是針對撥號使用者的身份確認與權限設定之用，特點是集中認證與授權的動作於一中心伺服器(centralized server)，避免將有關使用者安全與權限等級等資料分散於各個數據機伺服器(modem server)之上，集中式單一資料庫與認證中心的設計有助降低管理成本，也更容易確保資料庫的一致性與減少重複資料分散於各伺服器時的資源浪費。

RADIUS 採用以 UDP/IP 傳送的 client-server protocol 架構，它的特色是整個訊息的傳遞一定要由 client 端發起 request，server 端再回復 response 給 client 端，server 端無法主動送出訊息給 client 端，所有的 request 與 response 採用一對一對應(one-to-one mapping)，RADIUS 允許 server 與 client 分置於 internet 上的兩端，雙方以 UDP/IP 來承載 RADIUS 的 protocol 。

Diameter 非常類似於 RADIUS，也是採用集中認證與授權的機制。但是改以 TCP/IP 的方式的 peer-to-peer protocol 架構，允許 Authentication Server 主動送出認證訊息給其下的 Authenticator。在本論文中，我們基於 pre-authentication 需求的考量，以 Diameter 做為 AP 與 AAA server 以及 AAA server 與 AAA gateway 之間的協定會比較適合。

2.4 AAA server 與 AAA gateway

我們須要 AAA gateway 做為 AAA server 與 AuC/HLR (爾後簡稱 AuC)之間的橋樑，其中 AuC 為原本 cellular network 的認證和使用者記錄中心。一般而言 AAA gateway 會置於 cellular network 系統業者處，作為 cellular network SS7 網路與 Internet TCP/IP 網路間的橋樑，AAA server 則放置於 WLAN provider 業者的機房做為認證的中心，AAA gateway 與 AAA server 之間由於可以是透過 Internet 來連接的。

此外，我們先必需要瞭解 AP 與 AAA server 之間的關係以及 AAA server 與 AAA gateway 之間的關係是有所不同的，AP 與 AAA server 是認證機制上的 client-server 關係，MN 會將其 SIM 卡的資料經由 AP 向 AAA server 發出認證要求。而 AAA server 與 AAA gateway 或其背後的 AuC 則是視為資料庫系統上的 client-server 關係，雖然 AuC 掌握 SIM 內部的金鑰 Ki (Individual subscriber authentication key)、認證演算法 A3 及加密金鑰產生演算法 A8，但 AuC 僅依 AAA server 的需求來產生針對某張 SIM 卡的 triplet，再回傳給 AAA server 作為和 SIM 卡資料認證比對之用。每個 triplet 包括隨機亂數 RAND (RANDom number)、簽章回應 SRES (Signed RESponse)與加密金鑰 Kc (Cipher key)，圖 2-2 所示即為原本 GSM/GPRS 如何利用 SIM 來做認證與加密的工作。

AAA server 與 AAA gateway 之間必須存有一套安全機制來確保 AAA gateway 不會被入侵者以假冒 AAA server 身分對其進行資料收集或以竊聽的方式取得這些 triplet 的資料，因此其安全性必須特別考量。使用 RADIUS 或 Diameter 來傳送是廣為接受的方法，當然我們也可以採用其他的訊息認證與加密技術來完成 AAA server 與 AAA gateway 之間的資訊保護。

2.5 WEP (Wired Equivalent Privacy)與 TKIP

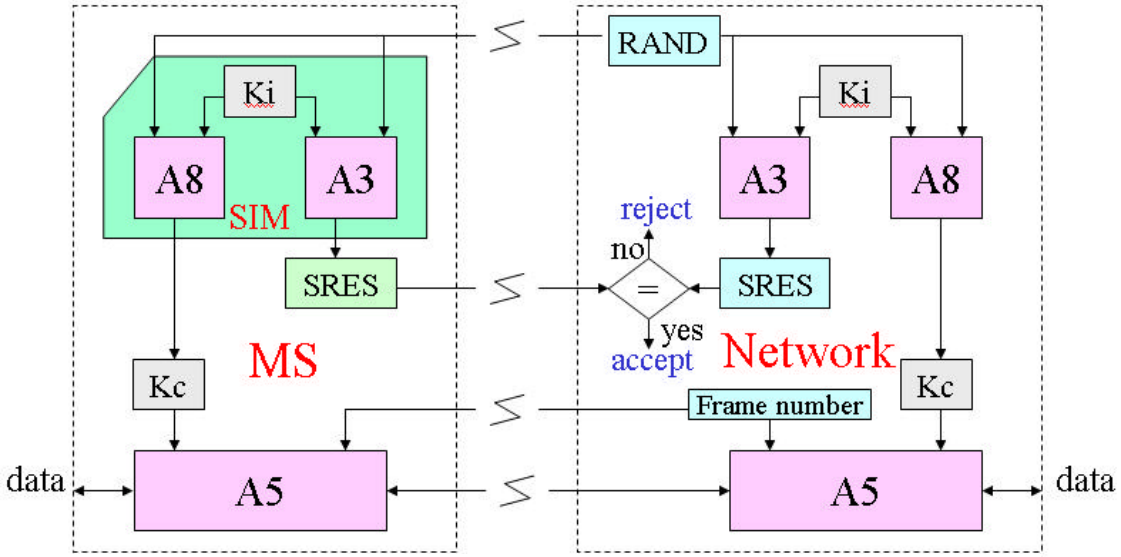

圖 2-2 GSM/GPRS SIM-based authentication and encryption

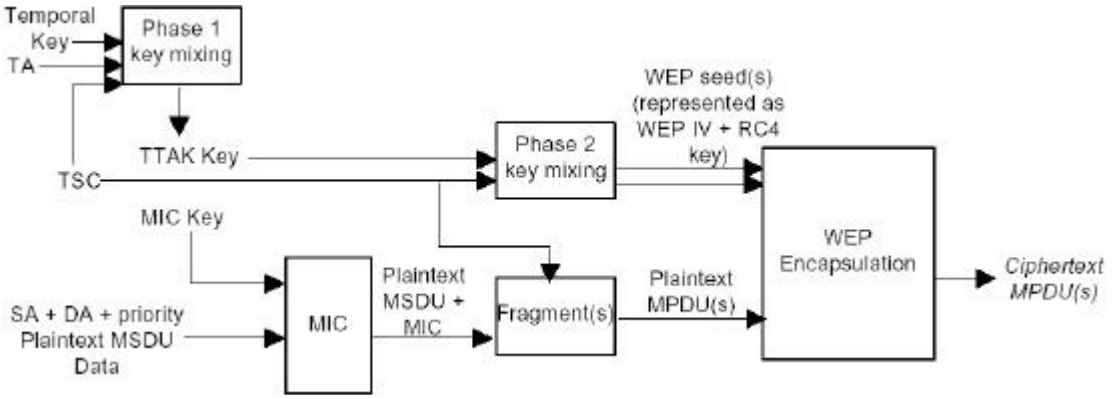

圖 2-3 TKIP Encapsulation Block Di agram

(Temporal Key Integrity Protocol)

有關 IEEE 802.11 WEP **的缺陷本論文裡不再做描述，可參考**[3][4]**得說明。為了強化** WLAN **無線端的安全，**IEEE 802.11 working group **決定採用新的加密安全機制** TKIP**。如圖** 2-3 **所示，**TKIP **是用新的** MIC algorithm- Michael **來加密原文** MAC PDU (MPDU)**，以取代原本** WEP **的** CRC-32 **運算，同時擴充的** IV (Initialization Vector)**欄位**- TSC (TKIP sequence counter)**可以避免** IV**太快發生重複而致使容易被猜到，另外以連續遞增的方式使用** IV **避免不預期的碰撞，最後** WEP RC4 **使用的金鑰與** IV **以及** MIC **使用的金鑰均先經過** key mixing function **動作來產生以必免** RC4 weak key **的攻擊，關於更多的** TKIP **技術部分請參考** IEEE 802.11i **相關文件**[9]**。**

這裡我們採用 TKIP **除了它解決了** WEP **的問題外，更重要的是我們需要它的** TSC **遞增的特性來做為再認證時機的依據，也是** MN **與** AP **雙方再認證後新舊金鑰更替同步的指示，這些將在下一章做更詳細的說明。**

三、Inter-AP fast handover 的快速認證機制

本論文以 IEEE 802.1x **的** port-based **為每個** MN **建立屬於自己的加密管道，透過** TKIP **的加密與** access control **技術為基礎，讓每個** MN **使用不同的金鑰傳送資料，另外我們採用有別於** IETF EAP-SIM draft [14]**的認證方式做** MN **與** WLAN **網路間的雙向認證與再認證動作，最後透過以主動式金鑰預先投遞** (key

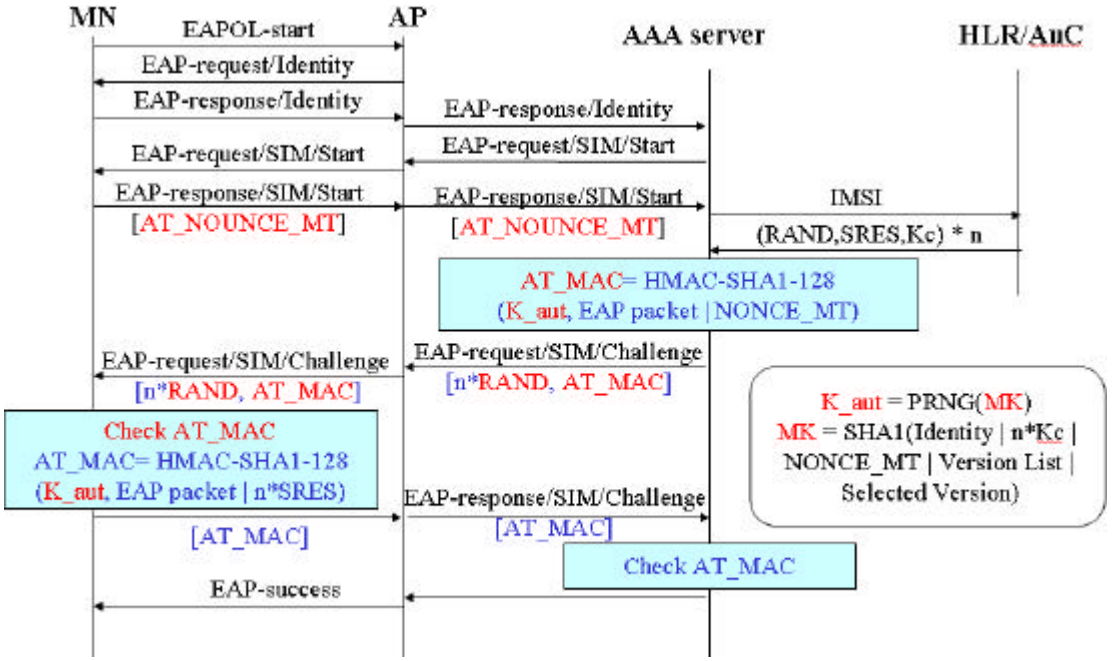

圖 3-1 EAP-SIM full-authentication message flow

pre-distribution)的先期認證技術幫助我們可以在不影響安全的前提下，減少不必要的再認證程序，進而減少 MN 在 inter-AP handover 時所花費的時間，因此研究的成果可以說是要達到支援 fast handover 目標的一個重要關鍵。整篇論文主要是整合認證程序、訊息完整性檢查、資料隱密與先期認證等四項技術來強固整個以 SIM-based 為基礎的 Public WLAN 環境。

3.1 MN 與 network 的雙向認證

IETF 的 EAP-SIM draft 當中使用由 AuC 傳來的多組 triplet 一次全部使用來產生一把主金鑰(MK; master key)，MN 隨機產生一個 NONCE_MT 來盤問(challenge)網路的合法性，網路端則一次利用多組的隨機亂數(RAND)來 challenge MN，雙方靠著這多組 RAND 所對應的 SRES 與 Kc 做認證的動作，圖 3-1 為一 EAP-SIM 做 full authentication 時的雙向認證動作。

上述 IETF EAP-SIM draft 中定義的 full authentication，其缺點在如有任何洩露的 triplet 將造成偽裝的網路的可能性，主因是所有的 RAND 均由 WLAN 網路端來決定，任何偽裝者僅要取得一組已知的 triplet 與 SIM 卡的 IMSI (International Mobile Subscriber Identity)即可偽裝成合法網路與 MN 溝通認證，因為偽裝者選用本身已知的 RAND、SRES 與 Kc，所以無論 MN 如何選擇 NOUNCE_MT，偽裝者都能計算出正確的 AT_MAC 來回應 MN。又由於 AAA server 與 AAA gateway 認證所須的 triplet 是透過不安全的 Internet 傳送，再加上 GSM 或 WLAN operator 內部有意或無意的外洩，抑或其他可能的情況都有可能造成少許的 triplet 洩露的情況發生，這些都有可能讓攻擊者利用低廉 WLAN 的相關設備來偽造網路端。更重要的是，原 SIM 卡所屬的 cellular network operator 將失去對 WLAN operator 的約束力，不管是合法或非法的 WLAN 業者僅要擁有 SIM 少數的 triplet 即可完全脫離 cellular network 的 AuC 認證而正常運作，WLAN 與 cellular network 業者之間的合法互信關係將受到嚴峻的考驗。

在此我們試著改變認證的方式，主要觀念是將原本 MN 對網路的 challenge，由僅對 WLAN AAA server 的 NOUNCE_MT，改為 MN 對 cellular network 的 AuC 提出 $RAND_M$，這個修改將迫使 AAA server 一定要向 AuC 取得一組由 $RAND_M$、$SRES_M$ 和 KC_M 所組成的 triplet 作為回應(AuC 將 $RAND_M$ 輸入 A3 和 A8 演算法分別求出 $SRES_M$ 和 KC_M)，以便進一步將 $SRES_M$ 回傳給 MN，完成 MN 對網路端的 challenge。特別值得注意的是：$SRES_M$ 的回傳是利用 piggyback 的方式，藉由網路端對 MN 的 challenge request 攜帶。此外，針對網路端對 MN 的 challenge，我們回歸 GSM/GRPS 的方法，使用一次一個 $RAND_N$ 的 challenge 方式去認證 MN 的合法性，MN 在收到 $RAND_N$ 後會計算出 $SRES_N$ 和 Kc_N，並將 $SRES_N$ 傳送到 AAA server 作比對。如此，經過上述 $RAND_M$ 與 $RAND_N$ 的一來一回，形成了一套嚴密安全的雙向認證機制，也同時完成了 Kc_M 與 KC_N 兩把加密金鑰的交換工作，這兩把各 64bits 的金鑰將組成長度 128bits 的金鑰做為 TKIP 加密時所使用的金鑰 (temporal key)，參考圖 2-3。

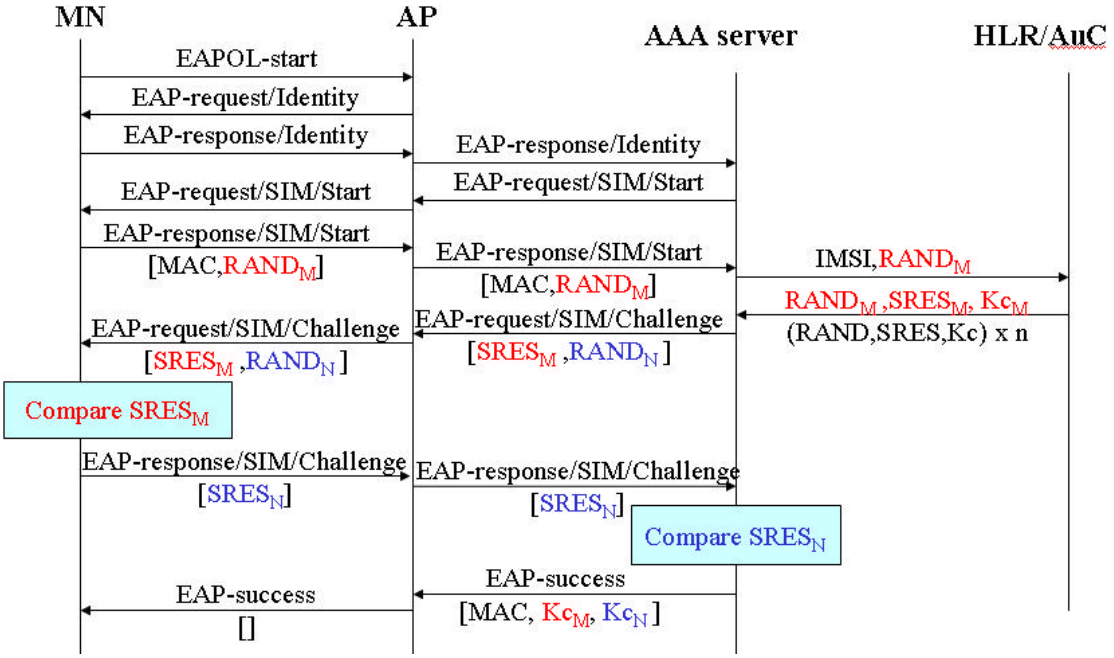

圖 3-2 New full-authentication message flow

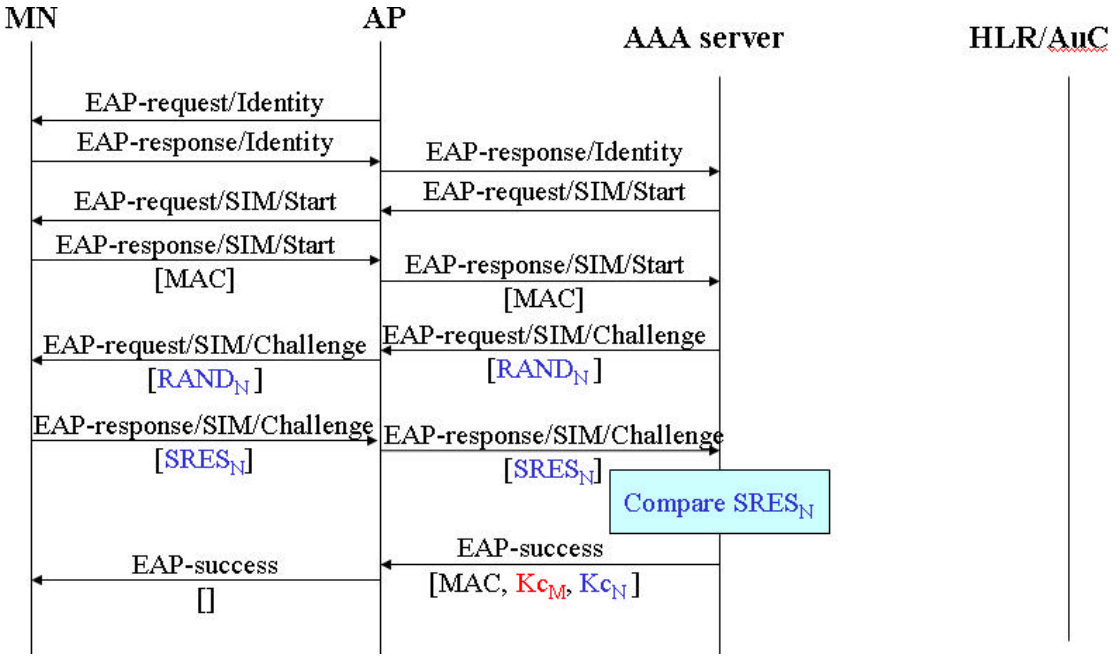

圖 3-3 New re-authentication message flow

由於 MN 自由選擇 $RAND_M$ 的方式，使得偽造的網路因無法計算對應於該 $RAND_M$ 的 $SRES_M$ 與 KC_M，缺少這組由 MN 選擇的 triplet，偽造者將難以通過後續的認證與未來的加密動作，如此一來也由於 $RAND_M$ 的存在將使 cellular network operator 對 WLAN operator 產生強迫性的約束力，WLAN 的 AAA server 少了 AuC 的回應將無法在 full authentication 獨立運作，不過目前的 HLR/AuC 必需經過些微的修改才能支援 $RAND_M$ 的 challenge。

3.2 MN 的再認證程序

一般而言，AuC 一次產生多組的 triplet 供 AAA server 使用，而在我們的方法中一次只使用一個 triplet 作 full authentication，其他未使用到的 triplet 將供未來 re-authentication 時使用，re-authentication 時我們採用單向認證的方法進行網路對 MN 的認證程序，如圖 3-3：

由於 re-authentication 時僅重新對 MN 做單向認證，我們依賴的是 KC_M 與 KC_N 兩把金鑰來進行後續的加解密與 WLAN 的存取控制(access control)，MN 與網路端會一直保留 KC_M 直到另一次的 full authentication 發生。雖然 re-authentication 僅更換其中一把金鑰，但是在認證時缺少其中的任一把都無法完成正確的加解密與 message integrity check。又雖然 MN 在 re-authentication 時為僅由網路端對 MN 進行的單向認證，但因只有合法的 AP 才能同時擁有兩把金鑰，偽裝者因無法取得原 KC_M 金鑰而仍無法成功偽裝成合法網路。

3.3 Inter-AP fast handover 快速換手的精神

以 IEEE 802.11 系列來看，整個 Inter-AP handover 的過程原本即要經過 probe、authentication 與 re-association 三個動作，如果再加上以 802.1x 的方式進行認證，需要在 re-association 之後再加上 IEEE 802.1x 的 EAPOL 認證(參考圖 1-1)。如果我們能利用 TKIP 附在每個封包上的 MIC 進行訊息認證即可有效防止未授權者非法使用入侵，也讓 MN 在 handover 時不需要再經過一次認證的動作。

圖 3-4 直接以訊息認證(Message Authentication)的方式與資料加密(Data Encryption)的方法來省略再認證的需要，這裡我們只要能使用一套足夠安全的 WLAN 安全機制(如 TKIP)來對往來的訊息進行檢查，過濾未經允許的封包通過。簡單的說，快速換手方法便是 MN 以換手不換鑰的方式進行不同 AP 間的 handover 動作，換言之，即是 MN 不因移動的關係而重新做認證的動作，MN 即使移動到新的 AP 之下仍會使用前一個 AP 時所使用的 KC_M 與 KC_N 這兩把組合金鑰來做為加解密與 message integrity check 的金鑰(請參考參考圖 2-3 及 802.11i TKIP 關於加密與訊息檢查[9])。圖 3-5 將說明 MN 通過舊 AP 的 IEEE 802.1x 認證後，即以相同的金鑰 access 另一個 AP。

參考圖 3-5，MN 在舊 AP 已經過認證後，即使換手到新的 AP 時，MN 會以已通過認證者的姿態在 probe 時即以設定 privacy bit (WEP bit)的方式通知新的 AP，當新 AP 檢視該 bit

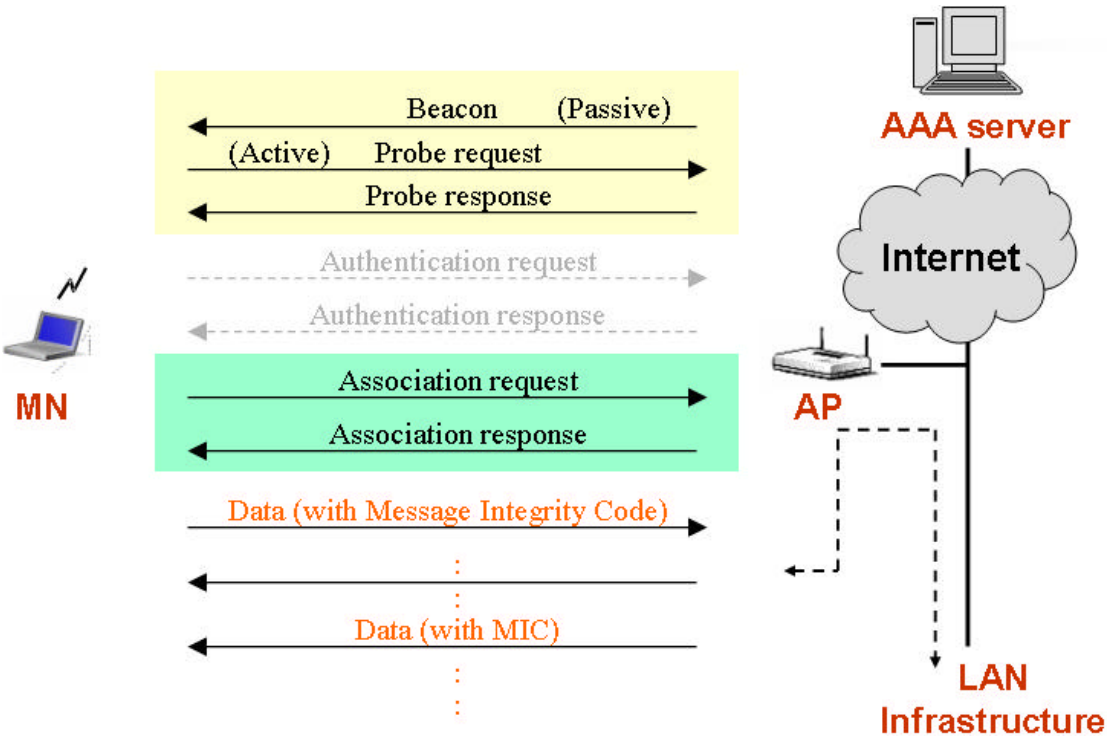

圖 3-4 Using message authentication to skip re-authentication procedure

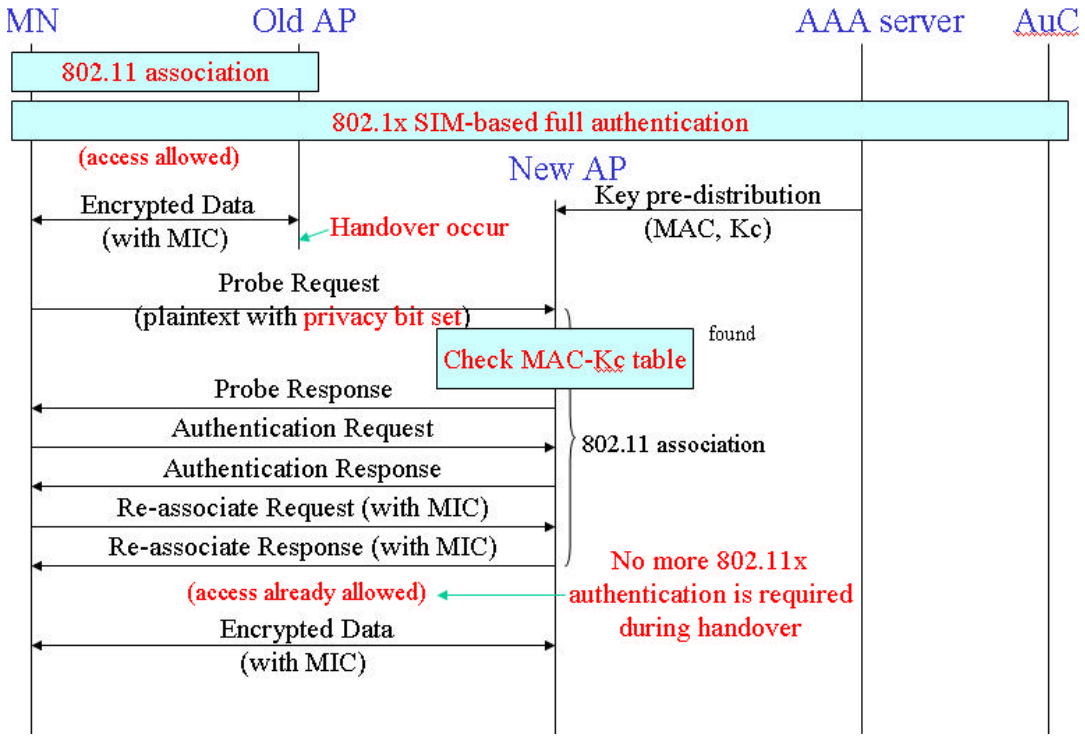

圖 3-5 MN handover without re-authentication required

被設定代表一個已經過認證的 MN 在進行 probe 動作，這將驅使 AP 查詢內部 MAC-KC table，如果金鑰不存在則須儘快向 AAA server 查詢該 MN 所使用的 KC 金鑰。圖 3-6 即假設 AP 並未事先收到 AAA server 的 key pre-distribution 訊息，此訊息帶有該 MN 的 MAC-KC 對照。因此當 MN probe AP 時，AP 儘快發出 key query 的 message 向 AAA server 查詢該 MN 的 KC 金鑰。圖 3-6 中也說明當 AP key missing 發生時，在 hold 與 cont.兩個 state 之間所產生的延遲. 這個延遲是肇因於有線網路上的單一封包傳送，所以實際上非常

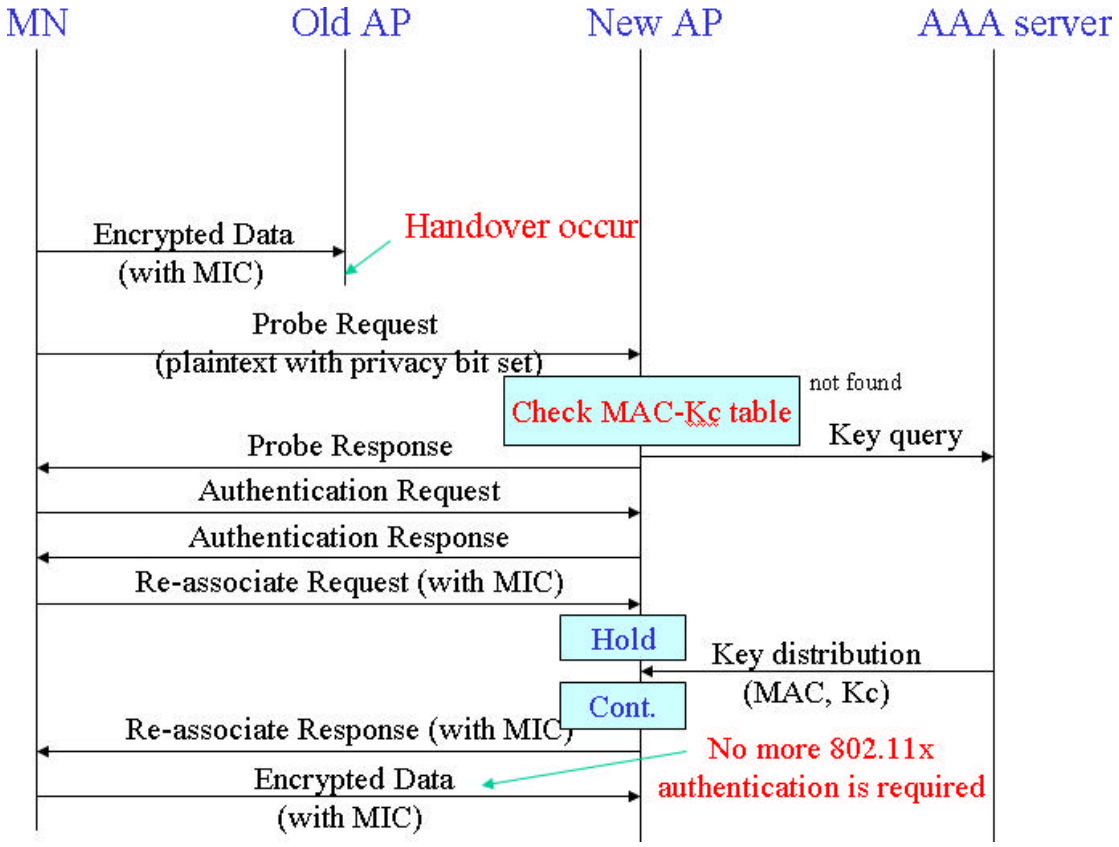

圖 3-6 MN handover with key missing delay

小，對 fast handover 的延遲要求影響不大。

實際上我們刻意在 re-associate request 放入 hold state，並強制 handover 的 MN 必需在 message 內加上 MIC code，能夠防止阻斷攻擊(DoS; deny of service)。因為只有當 AP 取回該 MN 金鑰並確認發訊者為該 MN 無誤，否則 AP 將不會處理該 re-associate request 的訊息。另外，由於 IEEE 802.11 的分散式系統在任何時間僅允許 MN 向單一個 AP 做 association，我們這樣做可避免攻擊者利用對其他 AP 發出 re-associate 的 message 來癱瘓合法使用者。

雖然上述機制已經提供一個安全的 inter-AP handover 環境，但是為了加強金鑰的安全性，不會因為金鑰長時間的使用，而有被猜出來的風險，我們也提供藉由 MN 的 re-authentication 取的新的金鑰。MN re-authentication 的時機將由 AP 負責掌控與發起，而 AP 則是完全依據 MPDU 的傳送個數(代表金鑰被使用的次數)來判斷是否已經達到一定的 threshold，作為 re-authentication 程序啟動的依據，而傳送個數可以利用 TKIP 加密演算法裡的 TSC (TKIP sequence counter)累積。由於每個 MN 擁有屬於自己的 TSC 空間，一旦 TSC 累計到達一定程度時，AP 便可單獨針對此特定的 MN 啟動 re-authentication 程序。

我們將 handover 與 re-authentication 的時機以非同步的方式進行，有別於以往 handover 與 re-authentication 須同步進行的方式，而將 handover 與 re-authentication 的時機錯開並不會影響安全性，並能確保金鑰的使用總時間或次數不會太長。如此設計的主因是，每一個 MN 的金鑰的使用次數和在不同的 AP 之間換手並沒有關係，而且如果不斷地因換手而造成 re-authentication 程序，對整個認證系統也是一種負擔。圖 3-7 描述 TSC 的累積過程，當 TSC 累積到 AAA server 設定給 AP 的 threshold 時，AP 主動發起再認證程序，整個再認證的動作可以完全在不中斷原本資料傳送的情況進行，一旦 MN 收到 EAP-success 的訊息後，以 reset TSC 的方式來讓雙方分辨新舊金鑰的交界，完成新舊金鑰的更替，如此可以不中斷資料的傳輸又不會造成新舊金鑰的混淆。

在每個 AP 內必須存有 MN 的 MAC-KC 的對照表，所以如果收到新的封包內 MAC address 不存在 MAC-KC table 時，將會驅使 AP 對 AAA server 進行該 MAC address 的 KC 金鑰查詢動作來更新 AP 內部的 MAC-KC table。如果 AAA server 內也未存有該 MAC address 的 entry 時，將由 AP 發起 full authentication 的程序。金鑰查詢(key query)的動作基本上只要一個來回的訊息交換，參與的對象只

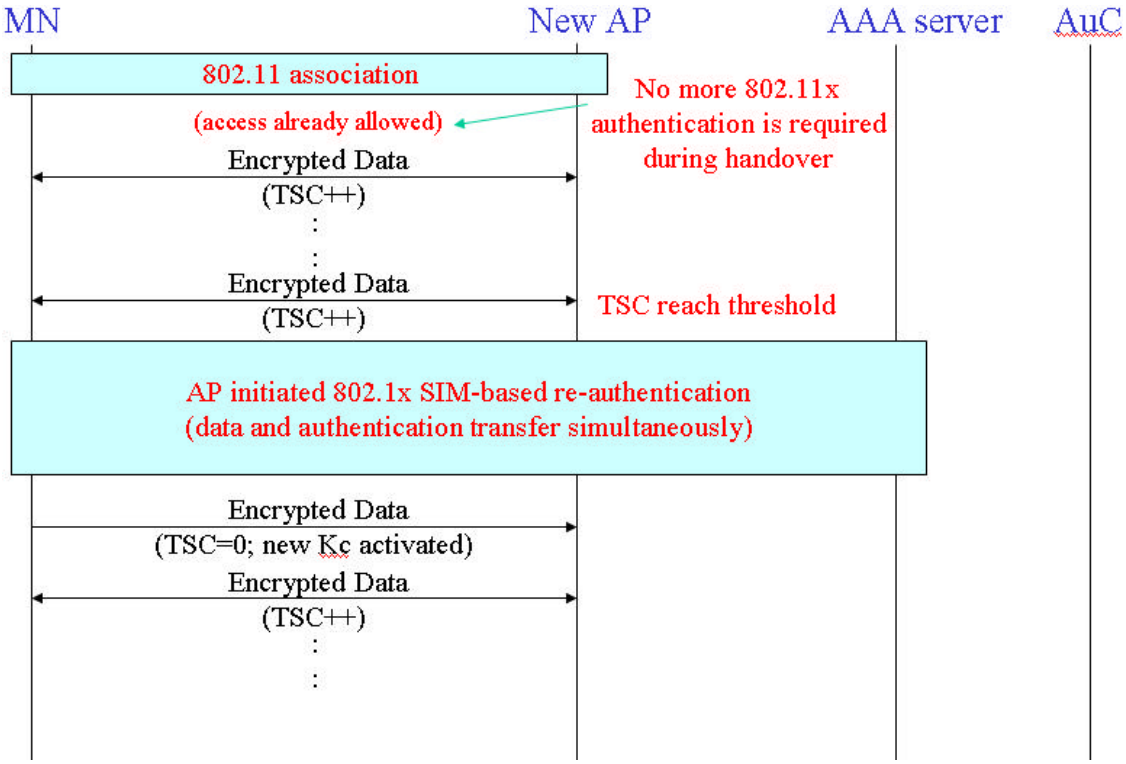

圖 3-7 TSC trigger AP initiates re-authentication procedure

限於 AP 與 AAA server 兩者，MN 則完全不須知情。比較 IEEE 802.1x 加上 EAP-SIM 的 re-authentication 則須要更多訊息交換，參與的對象包括 MN、AP 與 AAA server，我們的方法即使在沒有 key pre-distribution 的幫助下仍可比 EAP-SIM draft 所使用的方法更有效率，MN 的動作也更單純。

本質上，MN 採用屬於自己所專屬的獨立金鑰移動於不同 AP 之間的精神與 cellular network 的 BTS 間的 handover 是相同的，另外我們認證時產生的其中一把加密金鑰 KC_N 將為未來的 WLAN 與 GSM/GPRS 作快速跨系統(跨階層)換手，也就是 inter-system (inter-tier) handover，預先提供可能的解決方向。

3.4 金鑰先期投遞(Key pre-distribution)的方法

我們使用金鑰先期投遞 (key pre-distribution)的技術盡可能在 MN 尚未移動到下一個 AP 時即已將加密金鑰 update 到新的 AP 的 MAC-KC table 上，如此一來可以完全省略 key query 的延遲，真正達到快速的 handover 目標 key pre-distribution 的策略與方法大致可分成全面性的投遞(key flooding)與選擇性的投遞(select distribution)，key flooding 方法簡單但適合較小的規模使用，select distribution 則須要另一套 MN 的位置追蹤機制來決定金鑰該投向那些 AP，這一套 MN 的位置追蹤機制已超出本論文的研究範圍，所以關於 select distribution 的更進一步討論需要另文

select distribution 的更進一步討論需要另文討論之。

最後，解釋為何採用 Diameter 來取代 RADIUS 做為 AP 與 AAA server 之間的 protocol。真正的重要原因是因為 RADIUS 採用 client-server 的 protocol 架構，它限制訊息的發起必須由 client 端開始，如此一來我們將無法完成主動式金鑰先期投遞技術。此外為了保護 AAA gateway 不被偽裝者以假造的 AAA server 攻擊來竊取 SIM 卡的 triplet，RADIUS 對這個方向的保護也不夠。為了安全性的考量，Diameter 的 peer-to-peer protocol 架構更能符合整個認證架構的需求。

四、效能分析

參考圖 1-1 與圖 3-4，以 802.1x 架構下換手延遲是由 probe 延遲 (D1)、802.11 authentication 延遲(D2)、(re)association 延遲(D3)及 802.1x authentication 延遲(D4)所組合而成，其中的 D4 因為不僅為 802.11 無線兩端的傳輸還包括 internet AAA server 與 client 間的遠距離傳輸，因此通常大於 D1+D2+D3 的總合。本文所提出的方法即是要消弭 D4 延遲時間對即時應用(real-time application)的影響又要同時保有高度的安全性。綜合原始 802.11 WEP 認證與 802.1x 下 EAP-SIM draft 認證方式與本文 SIM based 認證方式與快速換手支援比較其換手延遲與缺點比較如下。

手延遲與缺點比較如下。

802.11 WEP **認證方式**:
handover delay time = D1+D2+D3

缺點: **安全方面不足**

EAP-SIM draft **認證方式**:
handover delay time = D1+D2+D3+D4

缺點: **在** public WLAN **環境下** D4 **換手延遲可能太長**

本論文 SIM based **認證方式與快速換手支援**:
handover delay time = D1+D3

優點: **可省略** WEP **認證**(D2)**與** 802.1x**認證**(D4)**的延遲且保有金鑰更新與** TKIP **的安全機制**

五、參考文獻

中文文獻之編號按姓名筆劃之順序，英文文獻請依姓氏字母順序排列，並請將中文列於前，英文列於後，範例如下:

[1] Arunesh Mishra, Minho Shin, and William Arbaugh, An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process (http://www.cs.umd.edu/~waa/pubs/handoff-lat-acm.pdf)

[2] Kaj J. Grahn, Goran Pulkkis, and Jean-Sebastien Guillard, Security of Mobile and Wireless Networks, June 2002.

[3] Nikita Borisov, Ian Goldberg, and David Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, July 2001. (http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html)

[4] W. A. Arbaugh, N. Shankar, and Y. J. Wan., Your 802.11 wireless network has no clothes. (http://www.cs.umd.edu/~waa/wireless.pdf)

[5] Yi-Bing Lin, and Imrich Chlamtac, Wireless and Mobile Network Architecture, pp. 164-165, 2001.

[6] ETSI ETS 300 929 (GSM 03.20 version 5.1.1) Security related network functions.

[7] IEEE Std 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[8] IEEE Std 802.1X Port-Based Network Access Control, 2001.

[9] IEEE Std 802.11i/D3.0, Wireless LAN Medium Access (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security, November 2002.

[10] IETF RFC 2104 HMAC: Keyed-Hashing for Message Authentication, February 1997.

[11] IETF RFC 2284 PPP Extensible Authentication Protocol (EAP), March 1998.

[12] IETF RFC 2865 Remote Authentication Dial In User Service (RADIUS), June 2000.

[13] IETF internet draft Diameter Base Protocol, December 2002. (http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-17.txt)

[14] IETF internet draft EAP SIM authentication, February 2003. (http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-10.txt)