公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96150292

※ 申請日期：96. 12. 26　　※IPC 分類：H04L 9/00
H04L 12/28

一、發明名稱：（中文/英文）

無線網路中執行換手程序的裝置與方法/

APPARATUS AND METHOD FOR EXECUTING THE HANDOFF PROCESS IN WIRELESS NETWORKS

二、申請人：（共 2 人）

姓名或名稱：（中文/英文）

1. 財團法人工業技術研究院/
   INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE
2. 國立交通大學/
   NATIONAL CHIAO TUNG UNIVERSITY

代表人：（中文/英文）

1. 林信義/LIN, HSIN-I
2. 吳重雨/WU, CHUNG-YU

住居所或營業所地址：（中文/英文）

1. 新竹縣竹東鎮中興路 4 段 195 號/
   195, SEC. 4, CHUNG HSING ROAD, CHUTUNG, HSINCHU, TAIWAN 31040
2. 新竹市大學路 1001 號/
   1001, TA HSUEH ROAD, HSINCHU CITY, TAIWAN 300

國　籍：（中文/英文）

1. 中華民國/R.O.C.　　2. 中華民國/R.O.C.

三、發明人：（共 2 人）

姓名：（中文/英文）

1. 林一平/LIN, YI-BING
2. 許世芬/HSU, SHIH-FENG

國籍：（中文/英文）

1. 中華民國/R.O.C.

2. 中華民國/R.O.C.

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

一種無線網路中執行換手程序的裝置與方法。此裝置包含一處理機執行一識別碼檢查機制，當無線網路用戶欲從一來源存取點移動至一目的地存取點時，無線網路用戶傳送一認證要求訊息至目的地存取點，識別碼檢查機制將認證要求訊息內的一 R0 金鑰持有者識別碼向此目的地存取點的一 R0KH 表查詢，並決定出正確換手程序的一設定參數，依此讓該無線網路用戶執行換手程序。目的地存取點之 R0KH 表是由在此目的地存取點網域範圍下可被其存取之所有 R0 金鑰持有者的識別碼來組成。

六、英文發明摘要：

Disclosed is an apparatus and method for executing the handoff process in wireless networks. The apparatus comprises a processor to execute an identification checking device. When a wireless network station wants to move from a source AP to a destination AP, the wireless network station sends an authentication request message to the destination AP. The identification checking device searches a R0KH table of the destination AP for the R0KH identifier contained in the authentication request message, and determines a setting parameter for executing a handoff process. Thereby, the wireless network station may execute the handoff process. A R0KH table of an AP consists of all identifiers of R0KHs that can be accessed by the AP.

七、指定代表圖：

(一)本案指定代表圖為：第五圖。

(二)本代表圖之元件符號簡單說明:

500 無線網路中執行換手程序之裝置	
501 無線網路用戶	515 R0KH 表
525 識別碼檢查機制	551 認證要求訊息
551a R0 金鑰持有者識別碼	555 設定參數
561 來源存取點	562 目的地存取點

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種無線網路(Wireless Network)中執行換手程序(Handoff Process)的裝置與方法。

【先前技術】

無線網路已是大眾連上網際網路(Internet)的重要媒介。無線網路通常比有線(Wired)網路容易被竊聽與盜用。於存取點(Access Point，AP)與無線網路用戶(Wireless Network Station)間，透過安全鑰匙(Security Key)來做認證(Authentication)與加密(Encryption)是無線網路的重大議題。如果存取點與無線網路用戶雙方沒有事先存放此安全鑰匙，則此鑰匙會在無線網路用戶連接上存取點時，使換手程序的執行產生。

由於執行換手程序需要耗費很多時間，可能導致即時性的應用程式中斷，例如網路電話(Voice over IP，VoIP)，IEEE 802.11r 通訊協定標準提出三階層金鑰(Three-Level Key)架構來加速換手程序的執行，並產生安全鑰匙。

第一圖是 IEEE 802.11r 通訊協定標準之三階層金鑰架構的一個範例示意圖。參考第一圖，第一層金鑰是配對主金鑰(Pairwise Master Key，PMK) R0，即 PMK-R0，

由第一層之萬用會議金鑰(Master Session Key，MSK)或AAA-金鑰(Authentication, Authorization and Accounting - key，AAA-key)所產生，並存放在無線網路用戶 101 與R0 金鑰持有者(R0 Key Holder，R0KH)中。MSK 是無線網路用戶執行換手程序時，與 AAA 伺服器(AAA Server)103 執行的 IEEE 802.1X 認證中，無線網路用戶 101 與 AAA 伺服器 103 各自產生。而 R0 金鑰持有者(R0KH)扮演 AAA 客戶端的角色接收並儲存從 AAA 伺服器 103 取得的 MSK。

第二層金鑰 PMK-R1 是存放在無線網路用戶 101 與 R1 金鑰持有者(R1KH)中，PMK-R1 是由第一層金鑰 PMK-R0 產生。PMK-R1 可用來產生第三層的配對暫時金鑰(Pairwise Transient Key，PTK)。此 PTK 就是無線網路用戶 101 與第三層內存取點間，訊息加密與解密使用的金鑰。

在前述 IEEE 802.11r 之三階層金鑰架構中，定義了移動網域(Mobility Domain，MD)架構。如第一圖所示，一個移動網域包含第一層 131 之多個 R0 金鑰持有者 R0KH；每一 R0 金鑰持有者(R0KH)具有多個 R1 金鑰持有者(R1KH)與其連結例如，$R1KH_1$ 與 $R1KH_2$ 直接和 $R0KH_1$ 連接，而 R1 金鑰持有者(R1KH)可以向移動網域內的所有 R0 金鑰持有者(R0KH)取得金鑰 PMK-R1，例如，

$R1KH_1$ 與 $R1KH_2$ 可以直接向 $R0KH_1$ 取得 PMK-R1，也可以向間接相連的 $R0KH_2$ 取得 PMK-R1，第二層 132 即為此多個 R1 金鑰持有者;第三層 133 是以下所描述之一個移動網域的所有存取點。

基於 IEEE 802.11r 通訊協定標準之移動網域架構，無線網路用戶的移動可分成移動網域內(Intra-MD)移動以及移動網域間(Inter-MD)移動。移動網域內移動又可以分成金鑰持有者內(Intra-R1KH)移動以及金鑰持有者間(Inter-R1KH)移動。例如，無線網路用戶 101 從存取點 AP_0 切換到存取點 AP_1 是 R1 金鑰持有者(R1KH)內(Intra-R1KH)移動;而從存取點 AP_1 切換到存取點 AP_2 或存取點 AP_3 是 R1 金鑰持有者(R1KH)間(Inter-R1KH)移動。此兩範例都是在同一網域 110 之範圍下的移動，是移動網域內移動。而移動網域間(Inter-MD)移動的範例如從移動網域 110 之存取點 AP_3 切換到移動網域 120 之存取點 AP_4。

無線網路用戶在移動網域內移動時，需要執行快速基本服務集(Fast Basic Service Set，Fast BSS)換手程序；而移動網域間移動時，需要執行初始移動網域連結(Initial MD Association)換手程序。透過存取點定時廣播探測(Probe)與標誌(Beacon)訊息中夾帶的移動網域識別碼(MD IDentity，MDID)可以分辨出是移動網域內移動或

是移動網域間移動。

目前移動網域識別碼可由各個服務提供者配置，然而無法保證不同服務提供者配置的移動網域識別碼不會重複。因此，如果無線網路用戶在移動網域間移動時，因為移動網域識別碼相同而誤判為移動網域內移動，而執行快速基本服務集(Fast BSS)換手程序。那麼換手程序執行到一半時，存取點會因為 R1 金鑰持有者(R1KH)無法向無線網路用戶使用的 R0 金鑰持有者(R0KH)取得 PMK-R1，進而無法產生配對暫時金鑰(PTK)，所以會去通知無線網路用戶結束執行快速基本服務集換手程序並執行初始移動網域連結換手程序。

第二圖與第三圖的範例流程示意圖分別說明無線網路用戶執行初始移動網域連結換手程序與快速基本服務集換手程序。

前述第一圖中，當無線網路用戶 101 開啟無線網路的功能，透過移動網域 110 的存取點 AP_1 連上無線網路，或是從另一移動網域 120 移動到存取點 AP_1 的範圍下時，從存取點 AP_1 廣播的探測與標誌訊息中得知為移動網域間移動，無線網路用戶 101 則執行第二圖中的初始移動網域連結換手程序。

在步驟 201A 與 201B 中，無線網路用戶 101 與存取點 AP_1 執行開放系統認證(Open System Authentication)流程。在步驟 201A 中，無線網路用戶 101 傳送認證要求(Authentication Request)至存取點 AP_1。在步驟 201B 中，存取點 AP_1 傳送認證回覆(Authentication Response)至無線網路用戶 101。開放系統認證的流程執行完後，存取點 AP_1 允許無線網路用戶 101 傳送 IEEE 802.11r 通訊協定的訊息至 AAA 伺服器。

步驟 202A 與步驟 202B 分別是連結要求(Association Request)與連結回覆(Association Response)。在步驟 202A 中，無線網路用戶 101 傳送連結要求訊息至存取點 AP_1，其中連結要求訊息中之移動網域資訊元素(Mobility Domain Information Element，MDIE)欄位設定為 "0"，代表無線網路用戶 101 支援快速基本服務集(Fast BSS)換手程序。在步驟 202B 中，存取點 AP_1 透過連結回覆訊息，將 $R0KH_1$ 與 $R1KH_1$ 與移動網域的識別碼(Identity)存放在移動網域資訊元素欄位回報給無線網路用戶 101。

在步驟 203 中，無線網路用戶透過存取點 AP_1 向 AAA 伺服器 103 執行 IEEE 802.1X 認證。此認證步驟成功後無線網路用戶 101 與 AAA 伺服器 103 各自產生萬用會議金鑰(MSK)，並且 AAA 伺服器 103 會將此金鑰傳送給 R0 金鑰持有者 $R0KH_1$。

在步驟 204A 與 204B 中，分別產生配對主金鑰 PMK-R0 與 PMK-R1。在步驟 204A 中，無線網路用戶 101 與 R0 金鑰持有者 $R0KH_1$ 分別執行金鑰推衍函數(Key Derivation Function，KDF)演算法，利用 R0 金鑰持有者 $R0KH_1$ 的識別碼和萬用會議金鑰(MSK)，與無線網路用戶的網路卡實體位址(MAC address)產生配對主金鑰 PMK-R0。在步驟 204B 中，利用此配對主金鑰 PMK-R0、無線網路用戶的網路卡實體位址以及 R1 金鑰持有者 $R1KH_1$ 之識別碼，產生配對主金鑰 PMK-R1。

在步驟 205 中，無線網路用戶 101 與存取點 AP_1 執行 IEEE 802.11i 的四向交握(4-way Handshake)，產生配對暫時金鑰 PTK。此步驟中，無線網路用戶 101 與存取點 AP_1 各自產生一個亂數“SNonce”與“ANonce”並交換。存取點 AP_1 將此兩亂數“SNonce”與“ANonce”、R0 金鑰持有者 $R0KH_1$ 的識別碼、無線網路用戶 101 的網路卡實體位址、以及存取點 AP_1 的網路卡實體位址傳送給 R1 金鑰持有者 $R1KH_1$。然後，無線網路用戶與 R1 金鑰持有者 $R1KH_1$ 分別執行金鑰推衍函數(KDF)演算法，並利用上述的參數與 R1 金鑰持有者 $R1KH_1$ 的識別碼和配對主金鑰 PMK-R1 產生配對暫時金鑰 PTK。產生配對暫時金鑰 PTK 後，R1 金鑰持有者 $R1KH_1$ 將此配對暫時金鑰 PTK 傳送給存取點 AP_1。

執行完上述的初始移動網域連結換手程序後，無線網路用戶 101 成功地與存取點 AP_1 進行資料傳輸與連線，並且 R0 與 R1 金鑰持有者 $R0KH_1$、$R1KH_1$ 會分別存放配對主金鑰 PMK-R0 與 PMK-R1。這兩把金鑰 PMK-R0 與 PMK-R1 可以再利用來產生新的配對暫時金鑰 PTK，因此省下耗時的 IEEE 802.1X 認證流程，減少換手程序的執行時間。

當無線網路用戶在同一移動網域 MD_1 範圍下移動時，例如，從存取點 AP_1 移動至存取點 AP_3，則可執行快速基本服務集(Fast BSS)換手程序，如第三圖的範例流程所示。

因為存取點 AP_1 與存取點 AP_3 在同一移動網域 MD_1，在步驟 301A 中，無線網路用戶透過快速轉換認證要求(Authentication Request)訊息，通知存取點 AP_3 要執行快速轉換(Fast Transition，FT)認證。此認證要求訊息中包含一個用來產生配對暫時金鑰 PTK 的亂數 SNonce，以及一個移動網域資訊元素欄位。此移動網域資訊元素欄位包括 $R0KH_1$、$R1KH_1$ 的識別碼與移動網域 MD_1 的識別碼(MDID)。

存取點 AP_3 從認證要求訊息的內容中得知 R1KH 間

(inter-R1KH)的切換發生了，回應一個認證回覆(Authentication Response)訊息給無線網路用戶 101，如步驟 301B 所示。此認證回覆訊息包含一個用來產生配對暫時金鑰 PTK 的亂數 ANonce，以及移動網域資訊元素欄位；此移動網域資訊元素欄位包含 $R0KH_2$、$R1KH_3$ 的識別碼與移動網域 110 的識別碼 MDID 等資訊。

無線網路用戶 101 在收到存取點 AP_3 的快速轉換認證回覆訊息後，利用亂數 ANonce 與移動網域資訊元素訊息，再藉由 $R1KH_3$ 的識別碼、無線網路用戶的網路卡實體位址與 PMK-R0，產生配對主金鑰 PMK-R1。此配對主金鑰 PMK-R1 會存放在無線網路用戶 101 與 $R1KH_3$ 內。再根據無線網路用戶的網路卡實體位址、存取點 AP_3 的網路卡實體位址、SNonce、ANonce、$R0KH_1$ 與 $R1KH_3$ 的識別碼產生配對暫時金鑰 PTK，如步驟 302 所示。如果無線網路用戶 101 從存取點 AP_1 移動到存取點 AP_0，由於此兩存取點連接到相同的 R1KH，則可以直接利用舊的 PMK-R1 來產生配對暫時金鑰 PTK。

如步驟 303 所示，存取點 AP_3 將無線網路用戶的網路卡實體位址、存取點的網路卡實體位址、SNonce、ANonce、及 $R0KH_1$ 識別碼等資訊傳送至 $R1KH_3$，來產生新的配對暫時金鑰 PTK。

在步驟 304 中，依據 $R0KH_1$ 的識別碼，$R1KH_3$ 向 $R0KH_1$ 要求新的 PMK-R1。但是，如果無線網路用戶 101 是從存取點 AP_1 移動到存取點 AP_0，則可省略此步驟。

取得新的 PMK-R1 後，$R1KH_3$ 執行 KDF 演算法，產生配對暫時金鑰 PTK 並傳送至存取點 AP_3，如步驟 305 所示。在此步驟後，無線網路用戶 101 與存取點 AP_3 都擁有相同的配對暫時金鑰 PTK。

無線網路用戶 101 與存取點 AP_3 執行步驟 306 之預留資源(Resources Reservation)與重新連結(Re-association)流程後，無線網路用戶 101 從存取點 AP_1 切換至 AP_3。如此，無線網路用戶 101 就可以開始使用存取點 AP_3 的服務。

在快速基本服務集(Fast BSS)換手程序中，是再使用 PMK-R0 來產生新的配對暫時金鑰 PTK 以加速換手程序。因為存取點會廣播探測(Probe)與標誌(Beacon)回應畫面(Response Frame)，並在回應畫面中夾帶存取點使用的 R0KH，R1KH，與移動網域(MD)三種識別碼，因此無線網路用戶在選擇好存取點之後，可以為移動網域內(Intra-MD)移動或是移動網域間(Inter-MD)移動來選擇適當的換手程序，特別是 MAC 位址可用來識別 R0KH 與 R1KH，而移動網域識別碼(MDID)由服務提供者(Vendor)

來管理。

【發明內容】

本揭露的實施範例中，提供了一種無線網路中執行換手程序的裝置與方法。不需要移動網域識別碼來執行換手，可排除移動網域識別碼的不確定性。在本揭露的技術中，每一存取點保有一 R0KH 表，此 R0KH 表記錄能被此存取點存取的所有 R0KH 的識別碼。

在本揭露的一實施範例中，可提供一種無線網路中執行換手程序的裝置，此裝置包含一處理機以執行一識別碼檢查機制。一目的地(Destination)存取點之 R0KH 表是由該目的地存取點在其網域範圍下可被其存取之所有 R0 金鑰持有者(R0KH)的識別碼來組成。當一無線網路用戶欲從一來源(Source)存取點移動至一目的地存取點時，無線網路用戶傳送一認證要求訊息至目的地存取點，識別碼檢查機制以認證要求訊息內的一 R0 金鑰持有者識別碼向此目的地存取點的 R0KH 表查詢，並決定出正確的換手程序的一設定參數，依此讓該無線網路用戶執行換手程序。

在本揭露的一實施範例中，可提供一種無線網路中執行換手程序的方法，可應用在無線網路用戶之移動，當一無線網路用戶欲從一來源存取點移動至一目的地存取

點時，該方法包含：無線網路用戶傳送一認證要求訊息至該目的地存取點，此認證要求訊息包含一 R0 金鑰持有者識別碼；以此 R0 金鑰持有者識別碼向該目的地存取點的一 R0KH 表查詢，以選擇一轉換程序，該目的地存取點之 R0KH 表是由此目的地存取點在其網域範圍下可被其存取之所有 R0 金鑰持有者的識別碼所組成；當此 R0 金鑰持有者的識別碼未存於此 R0KH 表時，執行一初始移動網域連結換手程序；以及當此 R0 金鑰持有者的識別碼已存於此 R0KH 表時，執行一快速基本服務集換手程序。

茲配合下列圖示、實施例之詳細說明及申請專利範圍，將上述及本發明之其他目的與優點詳述於後。

【實施方式】

本揭露的實施範例中，提出一種機制與方法，可讓存取點幫無線網路用戶選擇換手程序，也不使用移動網域識別碼，避免識別碼重覆的問題發生。本揭露中，每一個存取點儲存一個由 R0KH 識別碼組成的表(Table)，以下稱之為 R0KH 表。當無線網路用戶從一存取點移動至另一存取點時，可透過 R0KH 表的查詢，讓存取點幫無線網路用戶選擇正確的換手程序。此無線網路用戶的移動可以是移動網域內移動或是移動網域間移動。

以第一圖之 IEEE 802.11r 通訊協定標準之三階層金鑰架構範例為例，本揭露設計的 R0KH 表的內容可如第四圖所示。由於在第一圖架構範例中，移動網域 110 之 R0KH 識別碼持有者為第一層 131 之 $R0KH_1$ 與 $R0KH_2$，因此第四圖中移動網域 410 的每一個存取點，即 AP_0、AP_1、AP_2、AP_3，皆儲存一個由 $R0KH_1$ 識別碼與 $R0KH_2$ 識別碼組成的 R0KH 表 415。類似地，第一圖架構範例中，移動網域 120 之 R0KH 識別碼持有者為 $R0KH_3$，因此第四圖中移動網域 420 的每一個存取點，即 AP_4、AP_5，皆儲存一個由 $R0KH_3$ 識別碼組成的 R0KH 表 425。

每一個存取點備有此 R0KH 表的資訊後，就可不使用移動網域識別碼，而能讓存取點幫無線網路用戶來選擇換手程序。第五圖是無線網路中執行換手程序之裝置的一個範例示意圖，與本揭露的某些實施範例一致。

參考第五圖，此裝置 500 包含一個處理機(圖內未顯示)，來執行一識別碼檢查機制 525。當一無線網路用戶 501 欲從一來源(Source)存取點 561 移動至一目的地存取點 562 時，無線網路用戶 501 傳送一認證要求訊息 551 至目的地存取點 562，識別碼檢查機制 525 以認證要求訊息 551 內的一 R0 金鑰持有者識別碼 551a 向此目的地存取點 562 的 R0KH 表 515 查詢，並決定出一換手程序的一設定參數 555。R0KH 表 515 是由一目的地

(Destination)存取點在其網域範圍下可被其存取之金鑰R0的所有持有者(R0KH)的識別碼來組成。

例如，第六圖中，當無線網路用戶 501 欲從存取點 AP_2 移動至存取點 AP_3 時，則識別碼檢查機制 525 查詢 $R0KH_2$ 的識別碼已經儲存在存取點 AP_3 之 R0 金鑰持有者識別碼表，可決定出 FT 認證是換手程序的一個設定參數。反之，當無線網路用戶 501 欲從存取點 AP_2 移動至存取點 AP_4，則識別碼檢查機制 525 查詢 $R0KH_3$ 的識別碼並未儲存在存取點 AP_3 之 R0 金鑰持有者識別碼表，可決定出開放系統認證是換手程序的一個設定參數。

無線網路用戶 501 收到目的地存取點回傳的認證回覆訊息後，在回傳的訊息中，若設定參數是 FT 認證，則無線網路用戶 501 會執行快速基本服務集(Fast BSS)換手程序；若設定參數是開放系統認證，則無線網路用戶 501 會執行初始移動網域連結換手程序。

所以，第六圖的範例中，當無線網路用戶 501 於移動網域內移動時，例如從存取點 AP_2 移動至存取點 AP_3，在回傳的訊息中，設定參數是 FT 認證，因此無線網路用戶 501 會執行快速基本服務集換手程序。如果無線網路用戶 501 是於移動網域間移動時，例如從存取點 AP_2 移動至存取點 AP_4，在回傳的訊息中，設定參數是開放系

統認證，因此無線網路用戶 501 會執行初始移動網域連結換手程序。所以，無論無線網路用戶的移動是移動網域內移動或是移動網域間移動時，皆可執行適當的換手程序。

由於在移動網域範圍內之 R0 金鑰持有者的變動與更新較不頻繁，因此 R0KH 表 515 的內容可以透過 AP 管理系統，靜態或動態地設定在 AP 中。藉由 R0KH 表 515 查詢來儲存所有 R0 金鑰持有者的識別碼，透過存取點的管理系統讓無線網路用戶選擇換手程序。本揭露的範例架構因為不需要管理移動網域識別碼，所以不會因為移動網域識別碼重複的問題而造成執行錯誤換手程序。也可以應用在 IEEE 802.11r 通訊協定標準之無線網路平台中。

根據本揭露的範例架構，當一移動網域內之 R0 金鑰持有者有變動與更新時，可動態或手動地更新存取點內的 R0 金鑰持有者識別碼表。

第七圖進一步說明無線網路中執行換手程序之方法的一個範例示意圖，與本揭露的某些實施範例一致。參考第七圖的範例，無線網路用戶 501 成功地與來源存取點 561 進行資料傳輸與連線後，當無線網路用戶欲從來源存取點 561 移動至目的地存取點 562 時，目的地存取

點 562 時備有一 R0KH 表，此 R0KH 表儲存目的地存取點 562 在其網域範圍下可被其存取之所有 R0 金鑰持有者的識別碼。以下步驟 701 至步驟 704 進一步說明如何執行換手程序。

在步驟 701 中，無線網路用戶 501 傳送一認證要求訊息至目的地存取點 562。透過此認證要求訊息通知目的地存取點 562 要執行快速轉換(Fast Tansition，FT)認證。此認證要求訊息內包含一 R0 金鑰持有者識別碼資訊，但不需要包含移動網域識別碼(MDID)資訊。

在步驟 702 中，選擇轉換程序。透過查詢 R0 金鑰持有者的識別碼是否儲存於目的地存取點 562 之 R0KH 表中，來選擇轉換程序。目的地存取點 562 收到無線網路用戶 501 之認證要求訊息後，讀取訊息中的 R0 金鑰持有者識別碼，並與目的地存取點 562 之 R0KH 表比對，來決定無線網路用戶 501 是執行初始移動網域連結(Initial MD Association)換手程序(步驟 703)，或是執行快速基本服務集(Fast BSS)換手程序(步驟 704)。

當 R0 金鑰持有者的識別碼未存於目的地存取點 562 之 R0KH 表時，在步驟 703 中，目的地存取點 562 執行開放系統認證，並回傳認證回覆(Authentication Response)訊息給無線網路用戶 501。回傳訊息中，參數設定為開

放系統認證。無線網路用戶 501 收到此回覆訊息後，執行初始移動網域連結(Initial MD Association)換手程序。此初始移動網域連結換手程序如第二圖中所述，不再重覆。

當 R0 金鑰持有者的識別碼已存於目的地存取點 562 之 R0KH 表時，在步驟 704 中，目的地存取點 562 執行快速轉換認證，並回傳認證回覆(Authentication Response)訊息給無線網路用戶 501。回傳訊息中，參數設定為快速轉換認證。無線網路用戶 501 收到此回覆訊息後，執行快速基本服務集(Fast BSS)換手程序。此快速基本服務集換手程序如第三圖中所述，不再重覆。

如此，不需要移動網域識別碼來執行換手，就可排除移動網域識別碼的不確定性。並且透過查詢存取點儲存的 R0KH 表，無線網路用戶可以分辨出是移動網域內或是移動網域間移動，而選擇換手程序來執行。

惟，以上所述者，僅為本揭露之實施範例而已，當不能依此限定本發明實施之範圍。即大凡一本發明申請專利範圍所作之均等變化與修飾，皆應仍屬本發明專利涵蓋之範圍內。

【圖式簡單說明】

第一圖是 IEEE 802.11r 通訊協定標準之三階層金鑰架構的一個範例示意圖。

第二圖是一個範例流程示意圖，說明無線網路用戶執行初始移動網域連結。

第三圖是一個範例流程示意圖，說明說明無線網路用戶執行快速基本服務集換手程序。

第四圖是 R0KH 表的內容的範例示意圖，與本揭露的某些實施範例一致。

第五圖是無線網路中執行換手程序之裝置的一個範例示意圖，與本揭露的某些實施範例一致。

第六圖說明無線網路用戶於移動網域內移動或是移動網域間移動時，來源存取點與目的地存取點儲存 R0KH 表的範例示意圖，與本揭露的某些實施範例一致。

第七圖是無線網路中執行換手程序之方法的一個範例示意圖，與本揭露的某些實施範例一致。

【主要元件符號說明】

101 無線網路用戶	103 AAA 伺服器
110、120 移動網域	131 第一層
132 第二層	133 第三層
R0KH R0 鑰持有者	R1KH R1 金鑰持有者
$PMK\text{-}R0_1$、$PMK\text{-}R0_2$、$PMK\text{-}R0_3$ 配對主金鑰 R0	

$PMK\text{-}R1_1$、$PMK\text{-}R1_2$、$PMK\text{-}R1_3$、$PMK\text{-}R1_4$ 配對主金鑰 R1	
PTK_0、PTK_1、PTK_2、PTK_3 配對暫時金鑰	
AP_0、AP_1、AP_2、AP_3、AP_4、AP_5 存取點	
201A 開放系統認證要求	201B 開放系統認證回覆
202A 連結要求	202B 連結回覆
203 執行 IEEE 802.1X 認證	205 產生配對暫時金鑰 PTK
204A 產生配對主金鑰 PMK-R0	204B 產生配對主金鑰 PMK-R1
301A 快速轉換認證要求	301B 快速轉換認證回覆
302 產生配對主金鑰 PMK-R1	
303 網路卡實體位址、存取點的網路卡實體位址、SNonce、ANonce、及 $R0KH_1$ 識別碼等資訊傳送至 $R1KH_3$	
304 要求 PMK-R1	
305 產生配對暫時金鑰 PTK 並傳送至存取點 AP_3	
306 預留資源與重新連結流程	
410、420 移動網域	415、425 R0KH 表
500 無線網路中執行換手程序之裝置	
501 無線網路用戶	515 R0KH 表
525 識別碼檢查機制	551 認證要求訊息
551a R0 金鑰持有者識別碼	555 設定參數
561 來源存取點	562 目的地存取點
701 無線網路用戶傳送認證要求訊息至目的地存取點	

702 選擇轉換程序
703 目的地存取點傳送開放系統認證回覆至無線網路用戶，以執行初始移動網域連結換手程序
704 目的地存取點通知快速轉換認證回覆至無線網路用戶，以執行快速基本服務集換手程序

十、申請專利範圍：

1. 一種無線網路中執行換手程序的裝置，可應用在無線網路用戶之移動，當一無線網路用戶欲從一來源存取點移動至一目的地存取點時，該裝置包含一處理機，該處理機執行一識別碼檢查機制，該無線網路用戶傳送一認證要求訊息至該目的地存取點時，該識別碼檢查機制以該認證要求訊息內的一 R0 金鑰持有者識別碼查詢該目的地存取點的一 R0KH 表，並決定出一換手程序的一設定參數，依此讓該無線網路用戶執行該換手程序；其中該目的地存取點 R0KH 表是由該目的地存取點在其網域範圍下可被其存取之所有 R0 金鑰持有者(R0KH)的識別碼所組成。
2. 如申請專利範圍第 1 項所述之無線網路中執行換手程序的裝置，其中該換手程序是一種初始移動網域連結換手程序或是一種快速基本服務集換手程序之其中一種換手程序。
3. 如申請專利範圍第 1 項所述之無線網路中執行換手程序的裝置，其中該無線網路中每一個存取點儲存一個在其網域範圍下可被其存取之所有 R0 金鑰之持有者的識別碼組成的 R0KH 表。
4. 如申請專利範圍第 1 項所述之無線網路中執行換手程序的裝置，其中該認證要求訊息內的該 R0 金鑰持有者識別碼存於該 R0KH 表時，該換手程序的該設定參數是快速轉換認證。

5. 如申請專利範圍第 1 項所述之無線網路中執行換手程序的裝置，其中該認證要求訊息內的該 R0 金鑰持有者識別碼未存於該 R0KH 表時，該換手程序的該設定參數是開放系統認證。

6. 如申請專利範圍第 1 項所述之無線網路中執行換手程序的裝置，其中該裝置係應用於 IEEE 802.11r 協定。

7. 如申請專利範圍第 1 項所述之無線網路中執行換手程序的裝置，其中該無線網路用戶之移動是移動網域內移動或是移動網域間移動的其中一種。

8. 一種無線網路中執行換手程序的方法，可應用在無線網路用戶之移動，當一無線網路用戶欲從一來源存取點移動至一目的地存取點時，該方法包含：

該無線網路用戶傳送一認證要求訊息至該目的地存取點，該認證要求訊息包含一 R0 金鑰持有者識別碼；

以該 R0 金鑰持有者識別碼查詢該目的地存取點的一 R0KH 表，以選擇一轉換程序，該目的地存取點的 R0KH 表是由該目的地存取點在其網域範圍下可被其存取之所有 R0 金鑰持有者的識別碼所組成；

當該 R0 金鑰持有者的識別碼未存於該 R0KH 表時，執行一初始移動網域連結換手程序；以及

當該 R0 金鑰持有者的識別碼已存於該 R0KH 表時，執行一快速基本服務集換手程序。

9. 如申請專利範圍第 8 項所述之無線網路中執行換手程序的方法，其中該無線網路中每一個存取點儲存一個

在其網域範圍下可被其存取之所有 R0 金鑰之持有者的識別碼組成的 R0KH 表。

10. 如申請專利範圍第 8 項所述之無線網路中執行換手程序的方法，其中當該 R0 金鑰持有者識別碼未存於該 R0KH 表時，該目的地存取點於一認證回覆訊息中，將該轉換程序的一參數設定為開放系統認證。

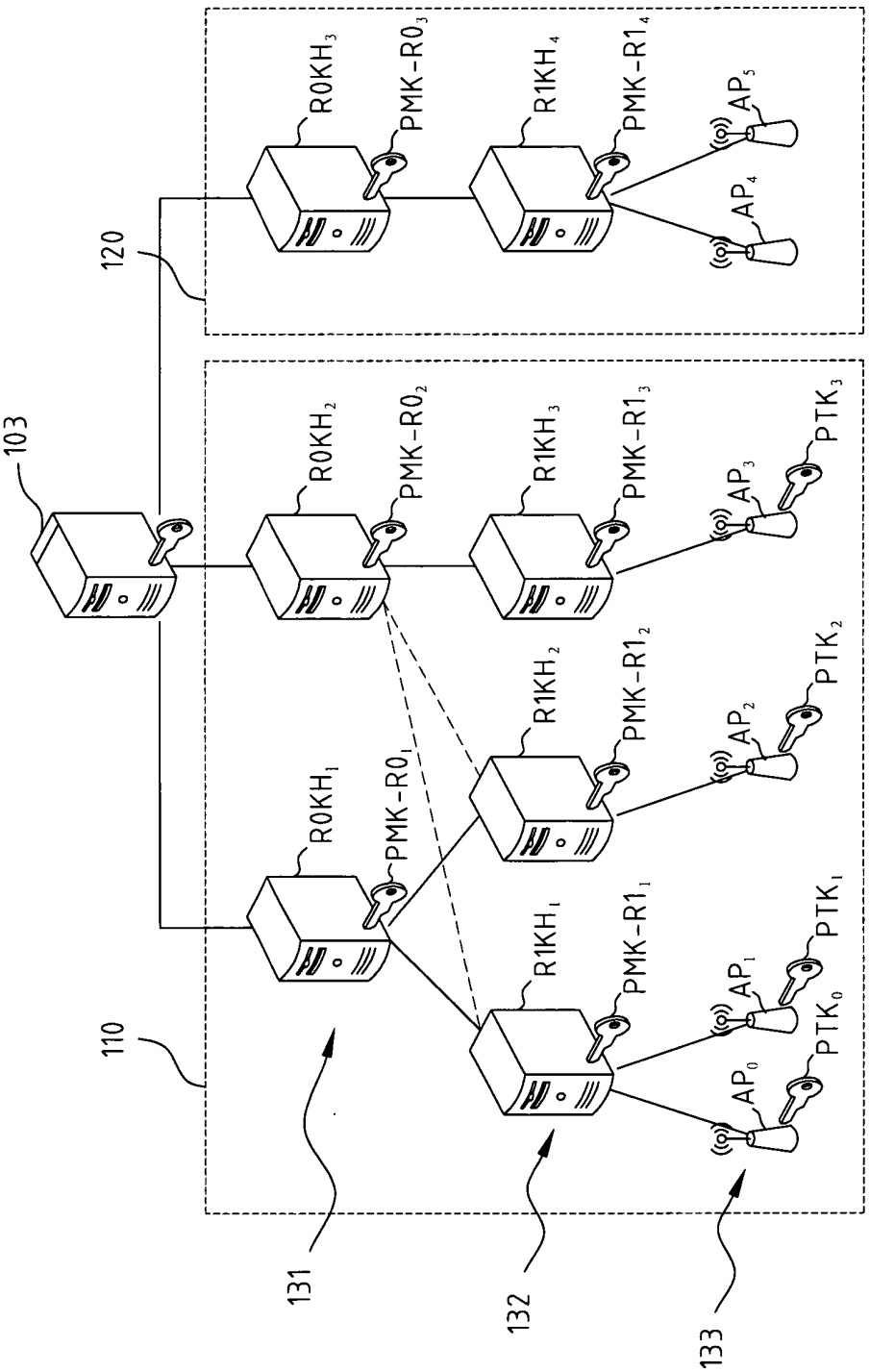
11. 如申請專利範圍第 8 項所述之無線網路中執行換手程序的方法，其中當該 R0 金鑰持有者的識別碼已存於該 R0KH 表時，該目的地存取點於一認證回覆訊息中，將該轉換程序的一參數設定為快速轉換認證。

12. 如申請專利範圍第 8 項所述之無線網路中執行換手程序的方法，其中該來源存取點與該目的地存取點在同一移動網域。

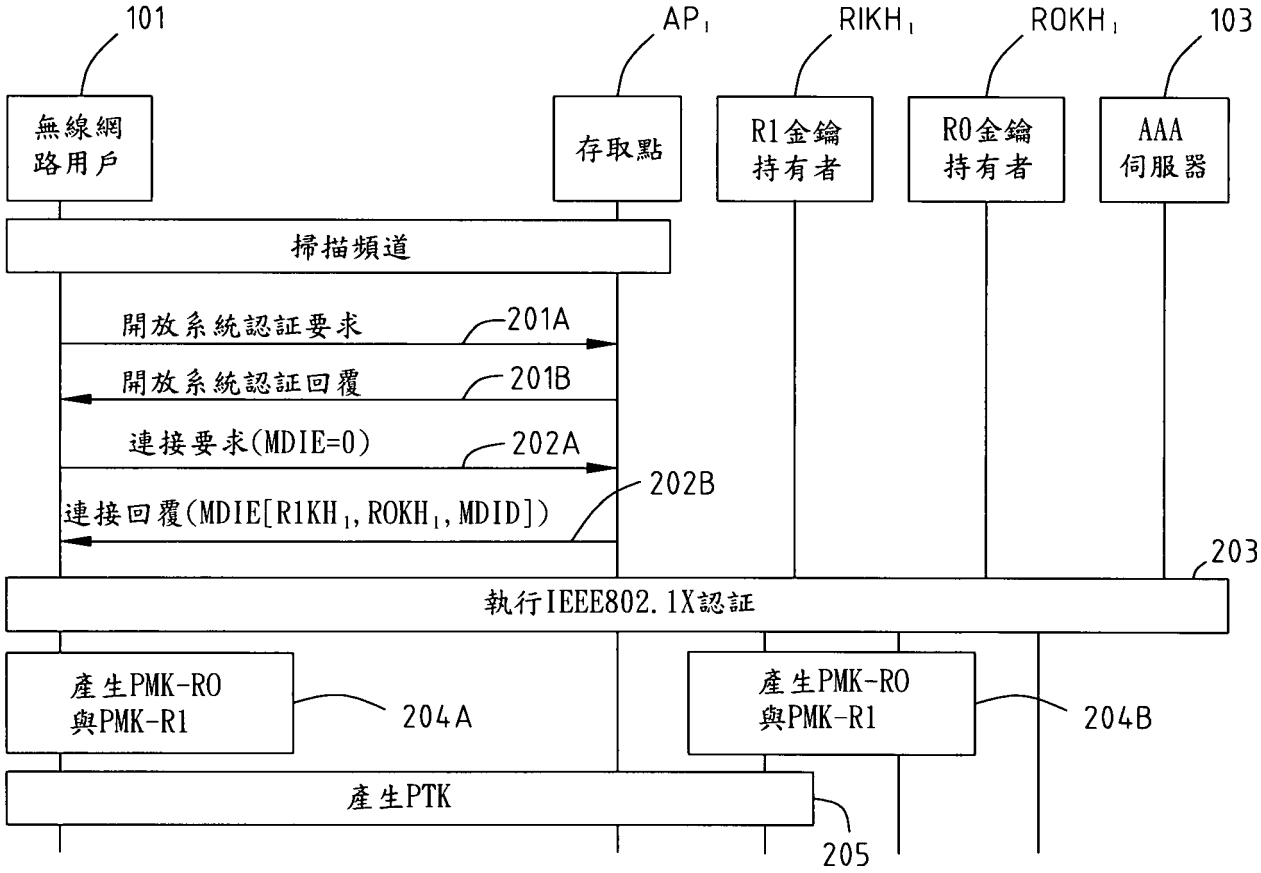
13. 如申請專利範圍第 8 項所述之無線網路中執行換手程序的方法，其中該來源存取點與該目的地存取點在不同的移動網域。

14. 如申請專利範圍第 10 項所述之無線網路中執行換手程序的方法，其中該無線網路用戶執行一初始移動網域連結換手程序。

15. 如申請專利範圍第 11 項所述之無線網路中執行換手程序的方法，其中該無線網路用戶執行一快速基本服務集換手程序。

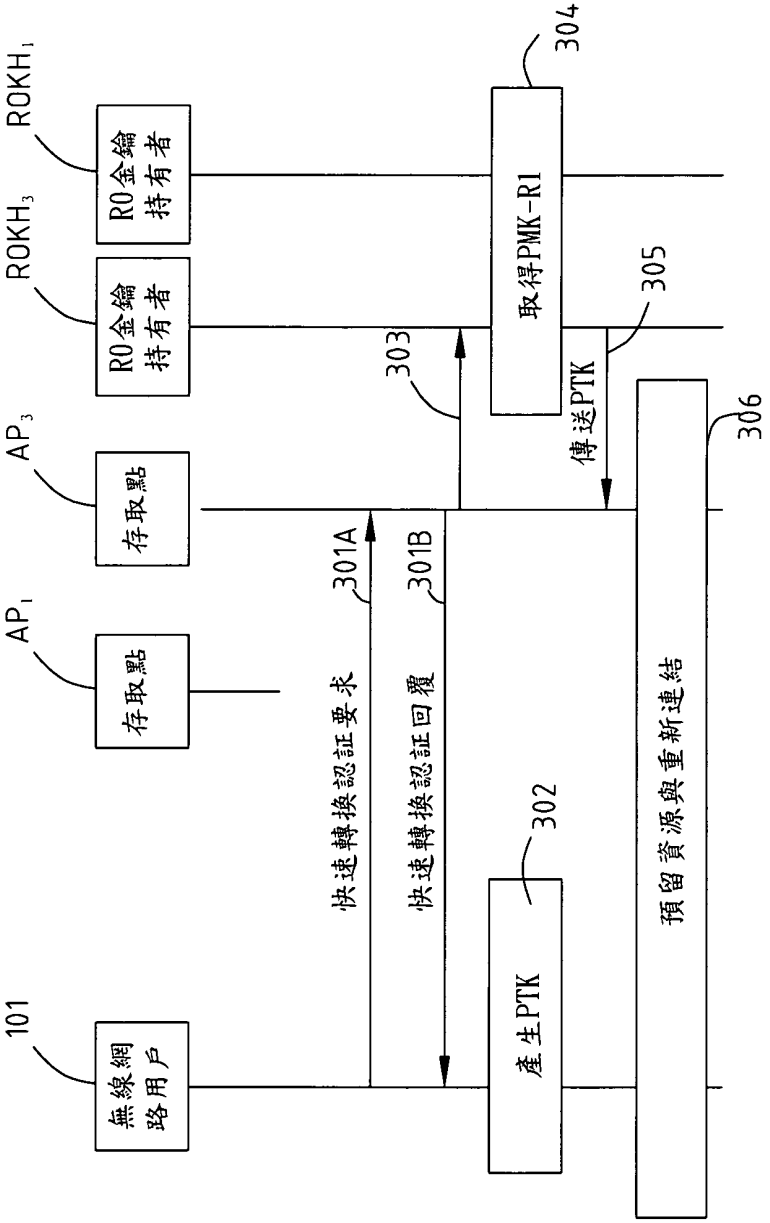

103
110
120
131
132
133
101
無線網路用戶
R0KH1
R0KH2
R0KH3
R1KH1
R1KH2
R1KH3
R1KH4
PMK-R0I
PMK-R02
PMK-R03
PMK-R11
PMK-R12
PMK-R13
PMK-R14
AP0
AP1
AP2
AP3
AP4
AP5
PTK0
PTK1
PTK2
PTK3
R0KH:R0金鑰持有者
R1KH:R1金鑰持有者
PMK-R0:配對主金鑰R0
PMK-R1:配對主金鑰R1
PTK:配對暫時金鑰
AP:存取點

第一圖（習知技術）

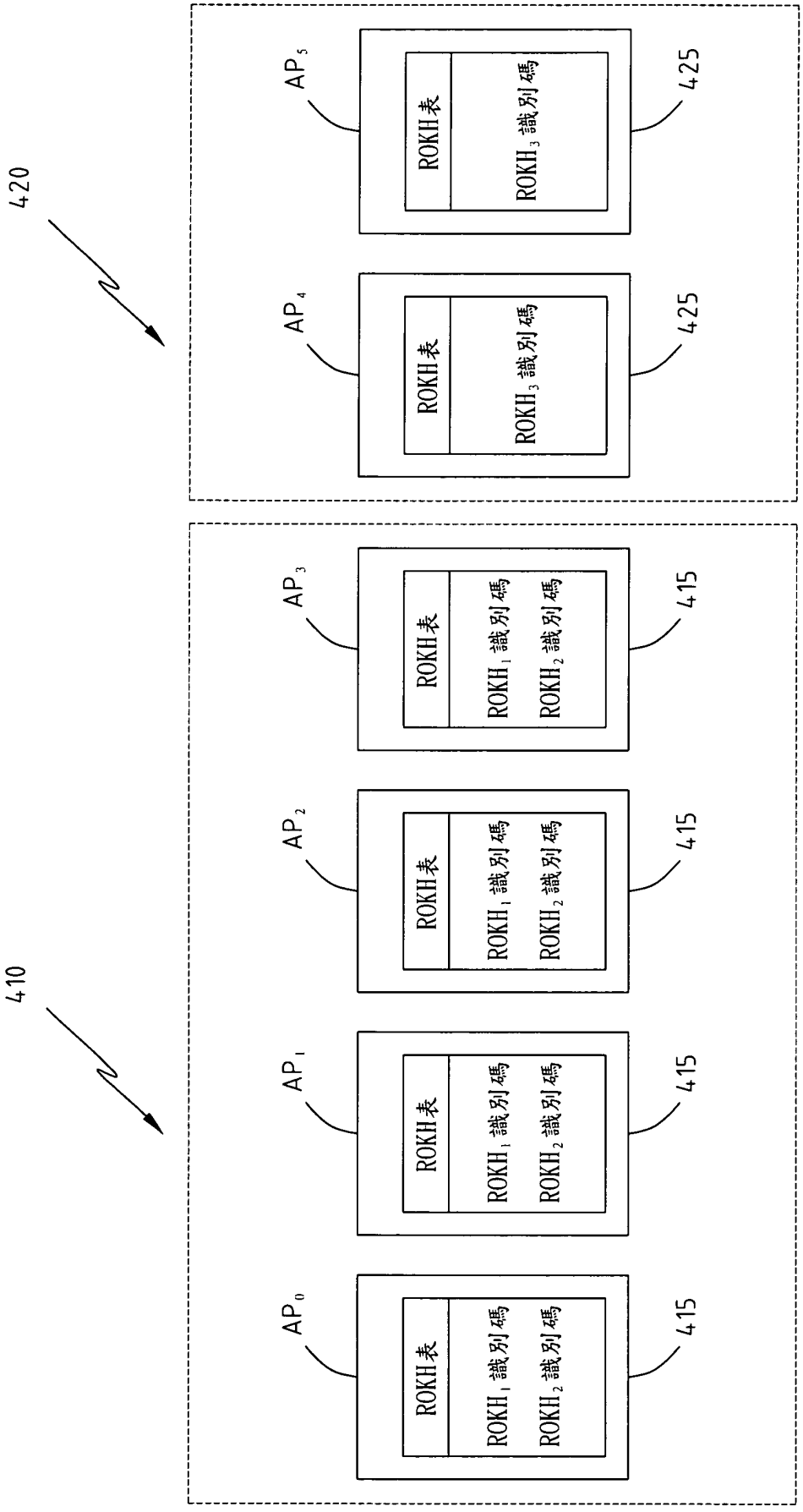


MDID:移動網域識別碼
MDIE:移動網域資訊元素

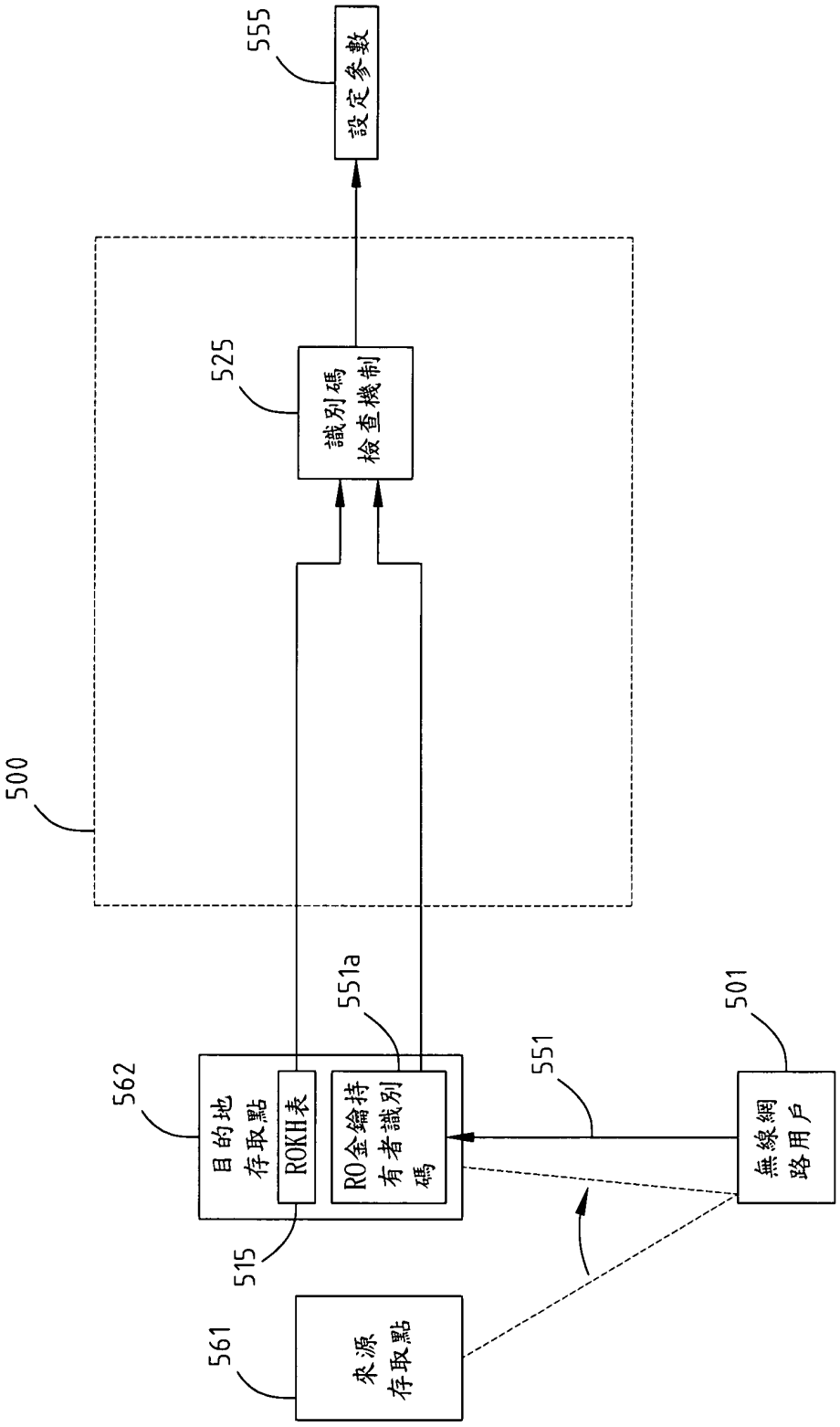
第二圖(習知技術)


101
無線網路用戶
AP1
存取點
AP3
存取點
ROKH1
R0金鑰持有者
ROKH3
R0金鑰持有者
快速轉換認証要求
301A
快速轉換認証回覆
301B
303
產生PTK
302
取得PMK-R1
304
傳送PTK
305
預留資源與重新連結
306

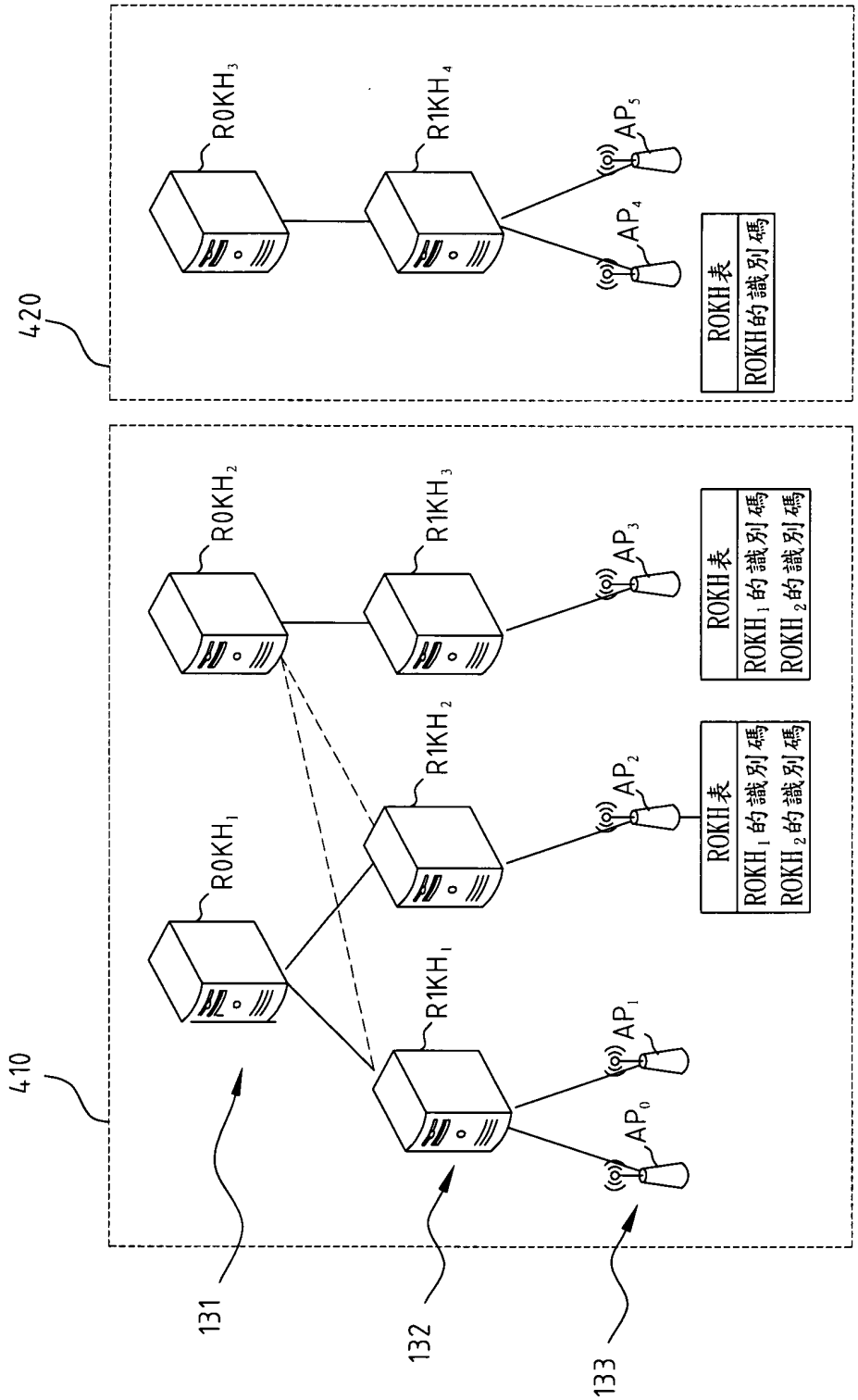
第三圖（習知技術）


410
420
AP0
AP1
AP2
AP3
AP4
AP5
ROKH表
ROKH1識別碼
ROKH2識別碼
ROKH3識別碼
415
425

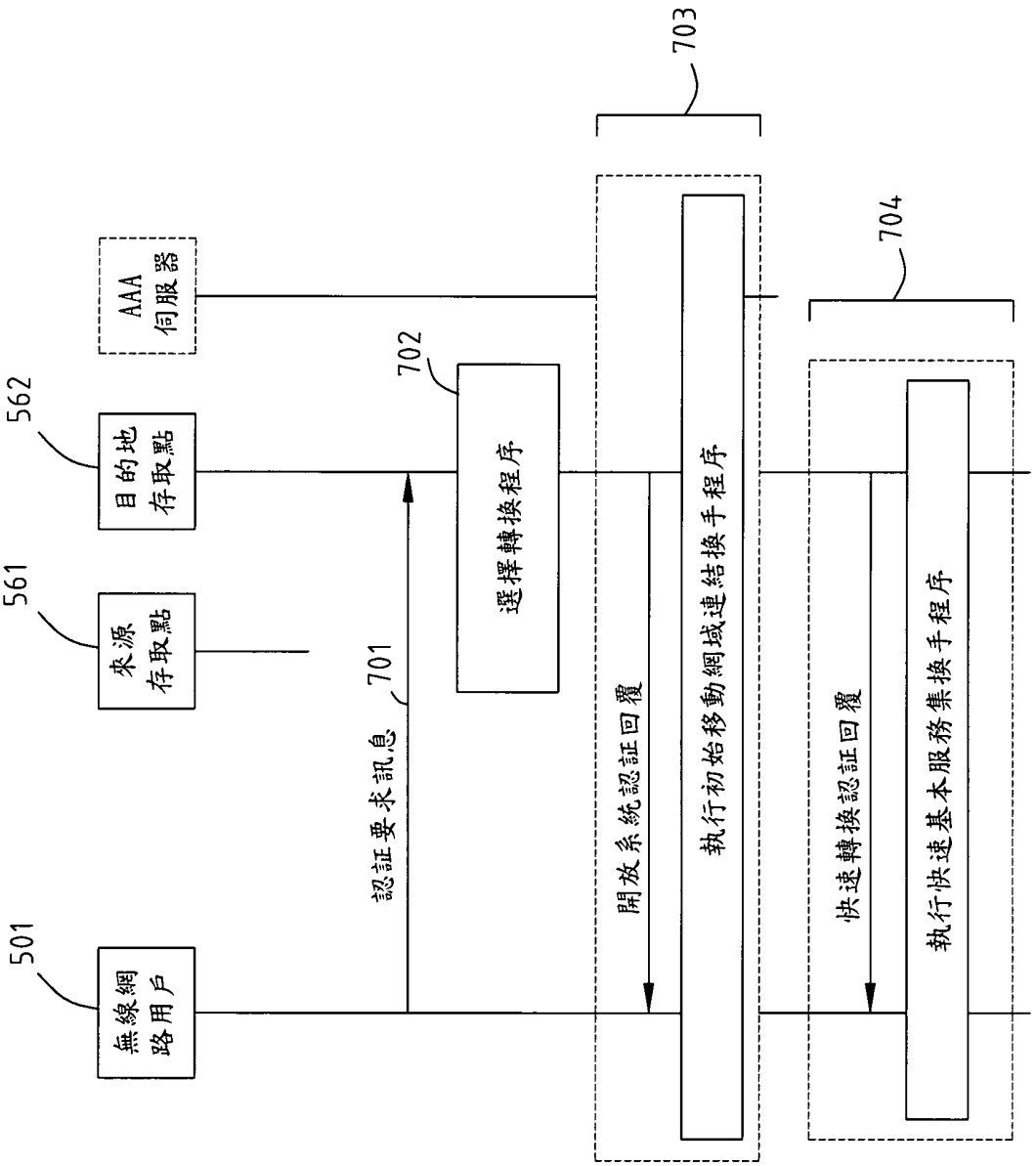
第四圖


555
設定參數
525
識別碼檢查機制
500
562
目的地存取點
ROKH表
RO金鑰持有者識別碼
551a
551
501
無線網路用戶
515
561
來源存取點

第五圖


410
420
R0KH1
R0KH2
R0KH3
R1KH1
R1KH2
R1KH3
R1KH4
AP0
AP1
AP2
AP3
AP4
AP5
ROKH表
ROKH的識別碼
ROKH1的識別碼
ROKH2的識別碼
131
132
133
501
無線網路用戶

第六圖


501
無線網路用戶
561
來源存取點
562
目的地存取點
AAA伺服器
認証要求訊息
701
702
選擇轉換程序
703
開放系統認証回覆
執行初始移動網域連結換手程序
704
快速轉換認証回覆
執行快速基本服務集換手程序

第七圖