公告本

100年12月7日修正替換頁

# 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：97133900

※ 申請日期：97.9.4　　※IPC 分類：H04L 29/06 (2006.01)
H04L 12/22 (2006.01)

## 一、發明名稱：（中文/英文）

提供安全通訊之方法、提供安全通訊之系統、中繼站、以及基地台

Methods and devices for establishing security associations and performing handoff authentication in wireless communications systems

## 二、申請人：（共 1 人）

**姓名或名稱：**（中文/英文）

財團法人工業技術研究院/
INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE

**代表人：**（中文/英文）蔡清彥/Ching-Yen Tsay

**住居所或營業所地址：**（中文/英文）

新竹縣竹東鎮中興路4段195號
No. 195, Sec. 4, Chung Hsing Rd., Chutung, Hsinchu 31040, Taiwan, R. O. C.

**國　籍：**（中文/英文）中華民國 TW

## 三、發明人：（共 2 人）

**姓　名：**（中文/英文）

1. 王瑞堂/ JUI-TANG WANG
2. 林咨銘/ LIN TZU-MING

**國　籍：**（中文/英文）

1. 中華民國 TW
2. 中華民國 TW

## 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】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國 US、2007/09/04、60/969,773
2. 美國 US、2007/10/22、60/981,767
3. 美國 US、2007/11/05、60/985,538
4. 美國 US、2008/09/03、12/203,652
5. 美國 US、2008/09/03、12/203,671

☐ 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：

一種提供安全通訊之方法，適用於在通訊網路上之基地台、中繼站、以及移動終端之間，此方法包括由中繼站接收來自移動終端之信號訊息；在接收信號訊息之後，由中繼站傳送安全金鑰請求至基地台；根據先前傳送之安全金鑰請求，由中繼站接收來自基地台之安全金鑰；以及由中繼站使用接收之安全金鑰來認證移動終端。

## 六、英文發明摘要：

A method of providing secure communications between a base station, a relay station, and a mobile station in a communication network is provided. The method comprises receiving, by the relay station, an unsolicited security key from the base station; receiving, by the relay station, a signaling message from the mobile station; and authenticating, by the relay station, the mobile station using the security key.

## 七、指定代表圖：

(一)本案指定代表圖為：第（ 6 ）圖。

(二)本代表圖之元件符號簡單說明:

104～AAA 伺服器；106～閘道器；206～IEEE 802.1X 完整認證程序；214～SA-TEK 三方交握程序；216～TEK 三方交錯程序；218～金鑰加密金鑰（KEK）；400～基地台；406～認證中繼站；414～移動終端；600～初始化程序；602～測距請求；604～移動終端認證請求；606～測距回應；608～對稱主金鑰(PMK)；610～認證金鑰（AK）；612～AK 傳送（金鑰請求及回應）；614～金鑰回應；616～資料加密金鑰(TEK)；618～訊息認證編碼金鑰(MACK)。

## 八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。

## 九、發明說明：

【發明所屬之技術領域】

本發明係有關於一種通訊系統，更特別是有關於一種在通訊系統中建立安全關聯以及執行交遞認證（handoff authentication）之系統及裝置。

【先前技術】

習知的無線網路環境連結行動電子裝置至服務供應商。更具體的來說，全球互通微波存取（Worldwide Interoperability for Microwave Access，WiMAX）的網路環境透過中介連接（intermediate connections）連結一用戶裝置至一網路。WiMAX 是一種無線網路科技，可以提供通信到相當遠的無線裝置。驗證與再驗證（reauthentication）造成的延遲，會使得與客戶端裝置（client device）通信的速度變慢，而且降低了 WiMAX 無線環境的效率。

第 1 圖為使用 IEEE 802.16d/802.16e WiMAX 無線通信系統的一習知無線通信系統的方塊圖。網路 100 提供給至少一個連線服務網路（Connectivity Service Network，CSN）102，連線服務網路 102 則使用至少一個認證、授權以及記錄（Authentication、Authorization、Accounting，以下簡稱 AAA）伺服器 104。CSN 102 連結到閘道器（gateway，GW）106 與 108。閘道器 106 與 108 為一種通信網路認證者（authenticator），通常是被連結到數個基地台（base station，BS）110 至 115，基地台的數量是取決於在一定區

域內的網路需求，雖然一個閘道器可能只能連結到單一的基地台，但一個閘道器仍可連結到多個基地台。在第 1 圖中只以閘道器 106 與 108 為例說明，但仍可視實際基地台的數量來決定使用更多或更少的閘道器。

在第 1 圖中，是以六個基地台為例說明 WiMAX 環境，但仍可視實際可使用的閘道器以及 WiMAX 網路需求來增加或減少基地台的數量。基地台，如基地台 110 與 104，用以與一個或多個客戶端裝置通信。客戶端裝置包括移動終端（mobile station，MS），如移動終端 120、122 以及 124，以及用戶終端（subscriber station，SS ）126 及 128，其中基地台提供無線網路服務給移動終端，且提供有線或無線網路服務給用戶終端。數個客戶端裝置的網路需求可能可以藉由單一基地台滿足，而單一基地台可能可以同時滿足移動終端與用戶終端的需求。

在習知的 WiMAX 網路環境中，如第 1 圖所示，每一次移動終端 120 被一閘道器，如閘道器 106，透過一相關的基地台，如基地台 110，初始服務時，都必需要對移動終端 120 進行認證。藉由這樣的認證動作，只要移動終端 120 移動的區域範圍內都能夠透過由原來認證的閘道器來使用服務的話，就不用對移動終端作更多的認證。但是，一但移動終端移到到一個區域，是由另一個閘道器提供服務，如閘道器 108，則閘道器在對移動終端 120 提供服務前，必須要先進行再認證動作。當一客戶端裝置被認證或在認證之後，安全關聯（security associations）或是兩個網

路實體，如移動終端 120 與基地台 110，之間的安全資訊會被建立，以確保兩者之間的通信安全。

認證協定標準（Authentication protocol standard）已經事先在認證技術上被標準化。這些標準化的協定可能包括，如 IEEE 802.1X 認證、GSM 用戶身份模組延伸式認證協定法（extensible authentication protocol method for GSM（global system for mobile communications） subscriber identity modules（EAP-SIM）），UMTS 用戶身份模組延伸式認證協定法與金鑰協議（extensible authentication protocol method for universal mobile telecommunications systems (UMTS) authentication and key agreement (EAP-AKA)）以及/或延伸式認證協定法與遠端認證撥接使用者服務協定（Remote Authentication Dial-in User Service，RADIUS）的一種組合。此外，標準化的交握協定，如安全關聯相關協定，可被使用來在一通信連結上建立複數個安全關聯，標準化的交握協定如安全關聯與資料加密金鑰三方交握程序（security association and traffic encryption key (SA-TEK) 3-way handshake procedure）與 TEK 三方交握程序。

在 IEEE 802.16d/802.16e WiMAX 無線通信系統，這些標準化的技術在一基地台與一移動終端之間執行。每一種標準化的認證技術需要多個傳輸（multiple transmissions），這會增加認證的時間以及處理所需的資源。

第 2 圖為 IEEE 802.16d/802.16e WiMAX 無線通信系統

中習知的認證與授權運作的信號流程圖。一初始化程序200被執行以確保移動終端的請求網路服務的請求被授權，使移動終端可以存取網路，且提供移動終端與基地台之的一安全關聯（security association），用以允許移動終端與基地台之間的的安全信息傳輸。舉例來說，當移動終端120從原先基地台110涵蓋的範圍移動到基地台111所涵蓋的範圍時，初始化程序200可能被使用以提供移動終端與基地台之的一安全關聯。

在初始化程序200的第1步中，移動端120是透過連接程序（link up process）無線連接基地台110，舉例來說連接程序包括一測距請求（ranging request）202與一測距回應（ranging response）204。移動終端120接著繼續認證程序的複數個步驟，認證程序可能如IEEE 802.1X完整認證程序206。AAA伺服器104計算一主會談金鑰（master session key，MSK）208給移動終端120，並將主會談金鑰208傳送給閘道器106，並儲存在閘道器106的快取中。這些認證程序的目的，如EAP認證方法或其他認證方法，就是要傳送已經傳送被AAA伺服器104、閘道器106以及移動終端120認證的MSK 208。閘道器106會先產生一對稱主金鑰(Pairwise master Key，PMK)210，再透過對稱主金鑰產生認證金鑰（authentication key，AK）212給移動終端120，並傳送AK 212至基地台111。

移動終端120可能會獨立的儲存與保留AK 212在自己的記憶體中，並且可能會產生AK 212。接著基地台111可

能執行 SA-TEK 三方交握程序（SA-TEK 3-way handshake procedure）214 去認證移動終端 212 保留的 AK 是與基地台 311 中的 AK 212 是相同的。使用 AK 212，一般是保留在基地台 11 與移動終端 120 中，可能可以分別的計算一訊息認證編碼金鑰（common message authentication code key，MACK）215 以及一金鑰加密金鑰（key encryption key，KEK）218。MACK224 可以分辨由移動終端 120 與基地台 111 產生的一認證訊息（authenticated message）。KEK 218 可以保護由移動終端 120 到基地台 111 的一資料加密金鑰（traffic encryption key，TEK）220。基地台 110 以及移動終端 120 可以使用 MACK 215 來執行 SA-TEK 三方交握程序 214 以便互相認證。當 SA-TEK 三方交握程序 214 被成功的執行完畢，基地台 110 產生 TEK 220 並且與 KEK 218 進行一 TEK 三方交錯程序 216，以建立與移動終端 120 的一安全關聯。TEK 220 一般來說是由基地台 111 亂數產生，且在移動終端 120 已經被認證且授權存取網路後，被使用來對傳輸在基地台 111 與移動終端 120 之間的資料加密。SA-TEK 三方交握程序 214 與 TEK 三方交錯程序 216 為習知技藝者所熟知，在此不贅述。

在使用在如第 2 圖的 IEEE 802.16d/802.16e WiMAX 無線通信系統中的初始化程序 200 中，基地台 111 控制基地台 111 與移動終端 120 之間是否有資料傳輸，這是因為基地台 111 與移動終端 120 都握有相同的 TEK 220、KEK 218、MACK 215、與 AK 212。當移動終端 120 已經建立與

基地台 111 的安全關聯後，換言之，移動終端 120 已經得到允許來透過網路通信，使用 TEK 220 的加密的資料傳輸也因此產生在移動終端 120 與基地台 111 之間。

請參考第 1 圖。當第 1 圖的系統運作時，信號的強度以及傳輸的品質可能會衰退，這是因為網路信號經過閘道器 106 或 108 至基地台 110-115 再到客戶端裝置所造成的。此外，當移動終端由原先提供服務的基地台移動到其他基地台的服務時，信號的強度以及傳輸的品質亦可能衰退。信號品質與覆蓋範圍可能會受到其他因素影響，如實體建築物、信號干擾、天氣以及傳輸條件與格式。因此，覆蓋間隙（gap）區域或漏洞（hole）區域可能會發生，而且當使用者位於這些區域時可能只有有限的或是根本沒有網路存取服務。

其中一個解決覆蓋間隙區域的方法就是提供更多的基地台，但這可能造成大量的成本花費。另外，為了避免這樣的問題，亦可以採用中繼站（relay station），如 IEEE 802.16j 中提到的多節點跳躍中繼網路協定技術（multi-hop relaying，MR）。基地台與中繼站之間的溝通只有在中繼站對來自基地台或移動終端的信號增強或中繼，並不會牽涉到認證程序或是建立安全關聯。

第 3 圖為使用 IEEE 802.16j WiMAX 且具有 MR 架構的通信系統的一習知通信系統的方塊圖。與 IEEE 802.16d 與 802.16e WiMAX 無線通信系統相似，透過至少一個 AAA 伺服器，如 AAA 伺服器 104，以及至少一個閘道器，如

閘道器 106，來存取網路 100。為了方便起見，網路 100、CSN 102、AAA 伺服器 104 與閘道器 106 被以核心網路（core network）300 表示。核心網路 300，或更精確的來說是閘道器 106，透過一有線連結來與基地台 310 至 313 通信。

在第 3 圖中，是以四個基地台為例說明，但是亦可以使用更多或更少數量的基地台。基地台，如基地台 310，一般是可以透過無線傳輸直接與一個或多個移動終端直接通信，如移動終端 320。基地台，如基地台 311 與 312，亦可間接與一個或多個移動終端通信。如移動終端 322、324、326。基地台一般可透過無線通信來與一個或多個中繼站通信，如中繼站 328、330 與 332，但也可以透過有線連接通信。中繼站 328、330 與 332 對於透過無線傳輸的方式，對於接收到來自或傳送到移動終端 322 的信號增強或中繼。如圖所示，中繼站 328、330 與 332 是固定的中繼站。但是，基地台亦可以與移動中繼站（mobile relay station，MRS）通信，如移動中繼站 334。移動中繼站可以駐在火車，飛機或其他機動運輸工具，用以提供擁有移動終端的乘客可以去透過移動中繼站來連結基地台或其他中繼來。如第 3 圖所示，移動中繼站 334 提供無線服務給移動終端 324 與 326，但單一移動終端或數個移動終端的網路需求可能可以透過單一移動中繼站得到滿足。雖然第 3 圖未表示，但是基地台，如基地台 310 至 313，可以與一個或多個用戶終端通信。因此，多個客戶端裝置的網路需求便可

以直接由單一基地台或是透過一個或複數個中繼站來滿足。更進一步來說，中繼站 328、330 與 332 可以提供無線服務給其他的中繼站、移動中繼站且/或移動終端。

在一些應用上，中繼站的使用可能會造成中繼站與基地台之間的台與台（station-to-station）交遞（handoff）需求的增加，而且因為每個中繼站（包括移動中繼站）有限的覆蓋區域，可能需要更多的處理資源來處理上述的台與台間的交遞。此外，當進行安全通信相關運作時，來自一中繼站或基地台到另一中繼站或基地台的交遞程序（handoff process）會消耗額外的資源，造成通信連接的效能、頻寬或品質降低。

【發明內容】

本發明提供一種提供安全通訊之方法，適用於在通訊網路上之基地台、中繼站、以及移動終端之間，此方法包括：由中繼站接收來自基地台未經請求之安全金鑰；由中繼站接收來自移動終端之信號訊息；以及由中繼站使用安全金鑰來認證移動終端。

本發明又提供一種提供安全通訊之方法，適用於在通訊網路上之基地台、中繼站、以及移動終端之間，此方法包括由中繼站接收來自移動終端之信號訊息；在接收信號訊息之後，由中繼站傳送安全金鑰請求至基地台；根據先前傳送之安全金鑰請求，由中繼站接收來自基地台之安全金鑰；以及由中繼站使用接收之安全金鑰來認證移動終端。

本發明又另提供一種提供安全通訊之方法，適用於在

通訊網路上之目標基地台、移動中繼站、以及至少移動終端之間，此方法包括：由移動中繼站傳送信號訊息至目標基地台，其中，信號訊息包括對應該至少一移動終端之訊息認證編碼（message authentication code，MAC）；由移動終端接收來自目標基地台之回應信號訊息；由移動中繼站接收來自目標基地台且對應至少一移動終端之至少一安全金鑰；以及由移動中繼站使用對應之安全金鑰來認證至少一移動終端。

本發明提供一種中繼站，用以在通訊網路上提供安全通訊，此中繼站包括至少一記憶體以及至少一處理器。記憶體用以儲存複數資料及複數指令。處理器用以存取記憶體。當處理器執行指令時該處理器根據接收自移動終端之信號訊息，使用接收自基地台之未經請求之安全金鑰來認證移動終端。

本發明又提供一種中繼站，用以在通訊網路上提供安全通訊，此中繼站包括至少一記憶體及至少一處理器。記憶體用以儲存複數資料及複數指令。處理器用以存取記憶體。當處理器執行指令時，處理器在接收來自移動終端之信號訊息之後，傳送安全金鑰請求至基地台，且根據先前傳送之安全金鑰請求，使用來自基地台之安全金鑰來認證移動終端。

本發明另提供一種基地台，用以在通訊網路上提供安全通訊，此基地台包括至少一記憶體以及至少一處理器。記憶體用以儲存複數資料及複數指令。一處理器用以存取

記憶體。當處理器執行指令時，根據移動終端進入至基地台之覆蓋區域內的指示，處理器將接收自認證、授權、及帳務伺服器之未經請求之主要金鑰傳送至中繼站。

本發明又提供一種基地台，用以在通訊網路上提供安全通訊，此基地台包括至少一記憶體以及至少一處理器。記憶體用以儲存複數資料及複數指令。處理器用以存取記憶體。當處理器執行指令時，根據接收自中繼站之安全金鑰，處理器將安全金鑰傳送至中繼站。

本發明另提供一種提供安全通訊之系統，包括基地台及中繼站。基地台用以提供對通訊網路之存取、認證在通訊網路上之移動終端、接收至少一安全金鑰、以及預先分發至少一安全金鑰。中繼站與該基地台通訊，用以接收預先分發之至少一未經授權之安全金鑰，且使用安全金鑰來提供安全資料傳送至認證之移動終端。其中，安全金鑰包括認證金鑰（authentication key，AK）及證明金鑰（verification key）中至少一者。

本發明又提供一種提供安全通訊之系統，包括基地台及中繼站。基地台用以提供對通訊網路之存取、認證在通訊網路上之移動終端、接收至少一安全金鑰、接收至少一安全金鑰請求、以及根據安全金鑰請求來傳送至少一安全金鑰。中繼站與基地台通訊，用以傳送至少一安全金鑰請求至基地台、根據安全金鑰請求接收來自基地台之至少一安全金鑰、以及使用安全金鑰提供安全資料傳送至移動終端。其中，安全金鑰包括認證金鑰（authentication key，

AK）及證明金鑰（verification key）中至少一者。

本發明另提供一種一種提供安全通訊之方法，適用於在通訊網路上之基地台、中繼站、以及移動終端之間，此方法包括根據來自中繼站之金鑰請求的接收，執行金鑰分發，以將對應移動終端之證明金鑰分發至中繼站；以及由中繼站執行金鑰證明，以識別移動終端。

本發明又提供一種提供安全通訊之方法，適用於在通訊網路上之基地台、中繼站、以及移動終端之間，此方法包括執行金鑰預先分發，以將對應移動終端之一未經請求之證明金鑰分發至中繼站；以及由中繼站執行金鑰證明，以識別移動終端。

本發明又提供一種提供安全通訊之方法，適用於在通訊網路上之基地台、中繼站、以及移動終端之間，此方法包括由中繼站執行金鑰證明，以識別移動終端；以及由移動終端執行金鑰證明，以識別中繼站。

為使本發明之上述目的、特徵和優點能更明顯易懂，下文特舉一較佳實施例，並配合所附圖式，作詳細說明如下。

【實施方式】

本案說明書中提及的實施例提供在 IEEE 802.16j WiMAX 無線通信環境或其他無線通信使用中繼站的網路系統內的複數個安全關聯。藉由提供可建立與一移動終端之間的安全連結以及可提供複數個移動終端存取網路 300 的中繼站，額外負擔（processing overhead）可以被顯著的

減少。特別是藉由提供具有資料加密金鑰（traffic encryption key，TEK）或訊息認證編碼（message authentication code，MAC）的中繼站，該中繼站可建立與移動終端的一安全關聯並且執行對移動終端的認證與授權，其中該 TEK 與 MAC 為對應想存取網路 300 的一移動終端。

第 4 圖為根據本發明之使用在 IEEE 802.16j WiMAX 無線通信系統的一無線通信系統的一實施例的方塊圖，其中該無線通信系統選擇使用中繼站作為認證中繼站（authenticator relay-relay station，AR-RS。或者又可以稱為 Access Relay Station，存取中繼站）。在第 4 圖中，一基地台（base station，BS）400 透過一有線線路連結到網路 300，並且比無線通信方式與一個或多個中繼站 402 與 404 通信，中繼站用以增強或中繼接收到的信號並傳送到複數個 AR-RS 406 至 409。如第 4 圖所示，AR-RS（MRS）408 為一移動中繼站（mobile relay station，MRS）。安全區域金鑰（security zone key），又稱中繼金鑰（relay key，RK），410 被基地台 400 散佈到中繼站 402 與 404 以及在中繼站 402 與 404 之後的 AR-RS 406 至 409，且 AR-RS 406 至 409 在對網路 300 的個別的初始化程序中被認證。安全區域金鑰被使用在 IEEE 802.116j 網路中的中繼站以及/或中繼站以及基地台之間的複數個通信通道（communication channels）的資料與信號的保護。中繼站 402 與 404 且/或基地台 400 可以使用中繼金鑰 410 來執行資料與信號的加

密、解密與訊息認證。由基地台 400、中繼站 402 與 404 以及 AR-RS 406 至 409 提供的網路覆蓋區域被稱為安全中繼區（security relay zone，SRZ）412。第 4 圖以由 AR-RS 406 提供服務的一移動終端（mobile station，MS）414 以及由 AR-RS（MRS）408 提供服務的移動終端 416 與 418 為例說明，但複數個移動終端的網路需求是可以由單一 AR-RS 所提供。此外，雖然圖上只有 AR-RS 408 表示為移動中繼站（MRS），在 SRZ 412 內額外的複數個 AR-RS 仍以作為移動中繼站。

每一次當移動終端 414 被初始化由基地台 400 提供服務時，都必需建立與網路 300 的一安全關聯(SA)。只要移動終端 414 在 SRZ 412 內移動，就可以繞過（bypass）進一步的安全關聯建立與認證。但是，一但移動終端 414 移到由另一個基地台提供服務的區域時，移動終端 414 就由其他基地台提供服務，如此一來就必需針對不同的基地台建立基地台與移動終端 414 之間的安全關聯(SA)，且取決於是否有其他的基地台被連結到閘道器（gateway，GW）106。對移動終端 414 的認證也是交遞（handoff）程序中的一部分。這樣的再認證且/或安全關聯建立程序，就造成對移動終端 414 提供服務的延遲。

第 5a 圖為一基地台的一實施例的方塊示意圖。基地台 400 可以為任何形式的通信裝置，用以在一無線通信系統中與一個或多個移動終端、中繼站以及/或 AR-RS，之間傳送且/或接收信號且/或通信，其中移動終端可能為移動終端

414，中繼站可能為中繼站402與404，AR-RS可能如AR-RS 406至409。如第5a圖所示，每一個基地台400可能包過一個或多個下列元件：至少一個中央處理單元（CPU）500、隨機存取記憶體（RAM）502、隨機唯讀記憶體（ROM）504、記憶體506、資料庫508、輸入/輸出（I/O）裝置510、介面512、天線514等。中央處理單元500用以執行電腦程式指令，以執行不同的程序與方法。RAM 502與ROM 504用以存取並儲存資訊與電腦程式指令。記憶體506用以儲存資料與資訊。資料庫508用以儲存複數個表（table）、目錄（list）或其他資料結構。上述元件為習知技藝者所熟知，在此不贅述。

第5b圖為一移動終端的一實施例的方塊示意圖。如圖所示，每一移動終端414可能包含一個或複數個下列元件：至少一個中央處理單元520、隨機存取記憶體（RAM）522、隨機唯讀記憶體（ROM）524、記憶體526、資料庫528、輸入/輸出（I/O）裝置520、介面522、天線524等。中央處理單元520用以執行電腦程式指令，以執行不同的程序與方法。RAM 522與ROM 524用以存取並儲存資訊與電腦程式指令。記憶體526用以儲存資料與資訊。資料庫528用以儲存複數個表（table）、目錄（list）或其他資料結構。上述元件為習知技藝者所熟知，在此不贅述。

第5c圖為中繼站或移動中繼站的一實施例的方塊示意圖。如第5c圖所示，每一中繼站或移動中繼站406可能包含一個或複數個下列元件：至少一個中央處理單元540、

隨機存取記憶體（RAM）542、隨機唯讀記憶體（ROM）544、記憶體 546、資料庫 548、輸入/輸出（I/O）裝置 540、介面 542、天線 544 等。中央處理單元 540 用以執行電腦程式指令，以執行不同的程序與方法。RAM 542 與 ROM 544 用以存取並儲存資訊與電腦程式指令。記憶體 546 用以儲存資料與資訊。資料庫 548 用以儲存複數個表（table）、目錄（list）或其他資料結構。上述元件為習知技藝者所熟知，在此不贅述。

第 6 圖係表示在 IEEE 802.16j WiMAX 無線通訊系統中認證及授權之信號示意圖，於此無線通訊系統中，被選擇之中繼站作為認證中繼站（AR-RS）。初始化程序 600 使用來保證需要網路服務之移動終端被授權來存取網路 300，以及為了安全訊息傳送而提供移動終端、中繼站以及 AR-RS 之間的安全關聯。舉例來說，在移動終端 414 剛開啟後，或在移動終端 414 由連接至閘道器 108 之基地台所提供之覆蓋區域移動至 AR-RS 406 所提供之覆蓋區域後，程序 600 用來認證且建立與移動終端 414 之間的安全關聯。首先，根據 IEEE 802.16 協定，移動終端 414 傳送信號訊息，例如測距請求（ranging request）602，至 AR-RS 406 以指示移動終端 414 位在 AR-RS 406 之範圍內。接著，又根據 IEEE 802.16 協定，AR-RS 406 藉由移動終端認證請求 604 來請求來自基地台 400 之認證，且傳送測距回應 606 至移動終端 414 以證實移動終端 414 之信號範圍以及測距請求 602 之接收。由於移動終端 414 無法事先或最近透過

基地台 400 與閘道器 106 來連接至網路 300，移動終端 414 藉由認證、授權以及記錄（Authentication、Authorization、Accounting，以下簡稱 AAA）伺服器 104 來執行 IEEE 802.1X 完全認證 206。由於 IEEE 802.1X 完全認證協定 206，閘道器 106 將接收來自 AAA 伺服器 104 之主會談金鑰（master session key，MSK），且接著自 MSK 取得且儲存對稱主金鑰(Pairwise master Key，PMK) 308 以及主要金鑰（master key），例如認證金鑰（authentication key，AK）610，給移動終端 414。主要金鑰（例如 AK 610）是來自可被取得之其他安全工具以及/或安全金鑰的鑰匙。接著，閘道器 106 安全地將 AK 610 傳送至基地台 400。在接收來自閘道器 106 之 AK 106 後，基地台 400 可直接將 AK 610 傳送至 AR-RS 406，以建立移動終端 414 與中繼站 406 之間的安全關聯。移動終端 414 可自己計算 MSK、PMK 608、以及 AK 610。

在一實施例中，為了允許 AR-RS 406 執行將來的認證協定以及建立與移動終端 414 間的安全關聯，基地台 400 傳送包括 AK 610 之金鑰回應 614 至 AR-RS 406。AR-RS 406 首先可自 AK 610 取得金鑰加密金鑰（key encryption key，KEK） 218 以及證明金鑰（verification key），例如訊息認證編碼金鑰（message authentication code key，MACK）618。接著，AR-RS 406 可與移動終端 414 在本地執行受 MACK 618 所保護的安全關聯與資料加密金鑰三方交握（Security Association and Traffic Encryption Key (SA-TEK)

3-Way Handshake）程序（以下稱為 SA-TEK 三方交握程序）214。當 SA-TEK 三方交握程序 214 成功地完成時，AR-RS 406 產生一隨機數字，以使用作為 TEK 616，且安全地傳送受 KEK 218 保護之資料金鑰（traffic key）（例如 TEK 218）至移動終端 414。最後，AR-RS 406 及移動終端 414 利用 TEK 616 來保護與 MACK 618 之間的資料傳送，以彼此認證。

第 6 圖係表示在 IEEE 802.16j WiMAX 無線通訊系統中認證及授權之信號示意圖，於此無線通訊系統中，被選擇之中繼站作為認證傳遞-中繼站（AR-RS）。此技術領域之人士能理解第 6 圖之 AR-RS 可以是移動中繼站，例如 AR-RS 408。此技術領域之人士也能理解，取代傳送 AK 610 至 AR-RS 406，基地台 400 可傳送不同之安全工具至移動終端，例如 AR-RS 406。例如，根據接收 AK 610，基地台 400 使用 AK 610 來產生 MACK 618，且傳送 MACK 618 至中繼站 406，以取代傳送 AK 610。中繼站 406 可使用 MACK 618 來認證或證明移動終端之身份。移動終端 414 及 AR-RS 406 可檢查酬載（payload）內的訊息認證編碼（message authentication code，MAC）或 MAC 封包之資料成分以彼此認證，藉此確認彼此。.

第 7 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 當前不持有要求的 AK。交遞程序 700 用來確保需要來自目標 AR-RS 之網

路服務之移動終端被授權來存取網路，以提供在移動終端與 AR-RS 之間的安全關聯，以允許安全訊息傳送。例如，交遞程序 700 使用來將移動終端 414 由 AR-RS 406 交遞至 AR-RS 407，其中，移動終端 414 先前已透過第 6 圖所述之程序且使用 AR-RS 406 而被認證。AR-RS 407 之記憶體（例如記憶體 546、ROM 544、RAM 542，或資料庫 548）當前不具有與移動終端 414 相關聯之 AK，例如 AK 610，但 AR-RS 406 及 AR-RS 407 都透過基地台 400 連接至網路 300。

在交遞程序 700 中，移動終端 414 首先傳送信號訊息（例如範圍要求 602）至 AR-RS 407，以指示移動終端 414 位在 AR-RS 407 之覆蓋區域內。範圍要求 406 可包括安全工具識別，例如移動終端訊息認證碼，HMAC 及/或 CMAC，其確認移動終端 414 是請求移動終端。認證金鑰識別（AKID）、MS MAC、HMAC、及/或 CMAC 之每一者將具有識別資訊之提供 AR-RS 407 提供給移動終端 414，且假使 AR-RS 407 沒有持有 AK 610 時可使用來請求來自基地台 400 之 AK 610。例如，假使 AKID 被包括，當 AR-RS 407 持有有效 AK，當 AR-RS 407 可決定認證對應的移動終端，或者當 AR-RS 407 非持有有效 AK，AR-RS 407 可請求來自基地台 400 之有效 AK。假使 AKID 沒有包括在測距請求 602 中，其他安全工具識別可用來證明被移動終端 414 所持有得 AK。由於 AR-RS 407 在其記憶體（例如記憶體 546、ROM 544、RAM 542，或資料庫 548）中非當

前具有 AK 610，AR-RS 407 傳送金鑰請求 704 至基地台 400。金鑰請求 704 包括對應移動終端 414 之 MAC/HMAC/CMAC。AR-RS 407 傳送測距請求 606 至移動終端 414，以證實移動終端 414 之存在以及測距請求 602 之接收。

根據金鑰請求 704 之接收，基地台 400 證明移動終端 414 之憑據。基地台 400 可自其記憶體（例如記憶體 546、ROM 544、RAM 542，或資料庫 548）中擷取 AK 610，且由於當移動終端 414 連接至 AR-RS 406 時，移動終端 414 先前已經歷了 IEEE 802.1X 完全認證 203 以獲得 AK 610，因此，對於基地台 400 與移動終端 414 而言，非必要再次經歷此程序。就其本身而論，基地台 400 傳送包括 AK 610 之金鑰請求 610 至 AR-RS 407，藉此給予 AR-RS 406 授權，以更進一步認證，且與移動終端 414 安全地通訊。

根據測距請求 606 之接收，移動終端 414 企圖使用延伸認證協定（extended authentication protocol，EAP）來初始化認證，以開始 IEEE 802.1X 完全認證 206。假使 AR-RS 407 接收一請求（例如支援 IEEE 802.16d 之私人金鑰管理延伸認證協定（privacy key management extended authentication protocol，PKM-EAP），或支援 IEEE 802.16e 之 PKMv2-EAP 之起使請求 708），AR-RS 407 可傳送 PKMv2-EAP 完整訊息 710 至移動終端 414，其將 IEEE 802.1X 完全認證 206 為成功的指示給移動終端 414，而不需實際經歷 802.1X 完全認證 206。

在 AR-RS 407 具有 AK 610 之後，其可執行與移動終端 414 之 SA-TEK 三方交握程序 214 或資料加密金鑰三方交握（TEK 3-Way Handshake）程序（以下稱為 TEK 三方交握程序）216，以建立與移動終端 414 之間的安全連接。在 TEK 三方交握程序 216 期間，AR-RS 407 可傳送新的資料金鑰給移動終端 414，例如由 AR-RS 407 所產生且使用 KEK 218 來加密的 TEK 712。AR-RS 407 及移動終端 414 接著透過安全通訊通道來聯絡。

第 8 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 透過未經請求的金鑰預先分發來接收指示。如第 8 圖所示，基地台 400 接收移動終端 414 即將進入或最近已進入至 AR-RS 407 之覆蓋範圍的指示。藉由使用額外信號訊息或預報技術（例如全球定位系統（GPS）），且透過 BS-BS 或 BS-閘道器通訊，基地台 400 接收來自另一基地台或來自閘道器 106 之此指示。由於當移動終端 414 連接 AR-RS 4006 時，移動終端 414 先前已經歷 IEEE 802.1X 完全認證 206 以獲得 AK 610，因此，對於基地台 400 與移動終端 414 而言，非必要再次經歷此程序。就其本身而論，基地台 400 傳送包括 AK 610 或者包括 TEK616 之未經請求的金鑰預先分發信號 802 至 AR-RS 407，藉此給予 AR-RS 407 授權且提供與移動終端 414 之安全通訊。此發生在移動終端 414 傳送信號訊息且 AR-RS 407 傳送金鑰請求之前，或者取代移動終端 414

傳送信號訊息且 AR-RS 407 傳送金鑰請求。接著，當移動終端 414 傳送測距請求 602 時，AR-RS 407 已經持有 AK 610 且簡單地執行 MAC 檢查（MAC Check）804，以證明被移動終端 414 所持有的金鑰，藉此證明移動終端 414 之識別。AR-RS 407 接著傳送包括 HMAC 或 CMAC 之測距回應 806。

在第 8 圖之實施例中，不僅透過 IEEE 802.1X 完全認證的淘汰，也透過 SA-TEK 三方交握程序 214 以及 TEK 三方交握程序 216 的淘汰，在當前 AR-RS 與目標 AR-RS 之間的交遞具有改善的效率。藉由提供具有 TEK 的 AR-RS 給先前認證之移動終端，對於先前認證之移動終端而言，可排除 SA-TEK 三方交握程序 214 以及 TEK 三方交握程序 216。特別的是，在一實施例中，目標 AR-RS 可接收來自當前 AR-RS 之 TEK，其中，此當前 AR-RS 先前已建立 TEK 給與移動終端 414 間之傳送。在另一實施例中，目標 AR-RS 接收來自基地台之 TEK，而其先前已透過與移動終端之間的直接傳送來建立基地台，或者以接收來自前一 AR-RS 之 TEK。因此，如第 8 圖所示，基地台 400 傳送 TEK 616 至 AR-RS 407，當作未經請求的金鑰預先分發 802 之一部分，或者是透過單獨的傳送。二者則一地，AR-RS 407 接收來自 AR-RS 407 之 TEK 616。假使 AR-RS 407 持有 TEK 616，其可跳過 SA-TEK 三方交握程序 214 以及 TEK 三方交握程序 216，藉此改善來自 AR-RS 407 之交遞之效率。一旦 AR-RS 407 獲得來自 AR-RS 407 之 TEK、來

自基地台 400 之 TEK，或者獲得藉由透過 SA-TEK 三方交握程序 214 以及 TEK 三方交握程序 216 來自己產生新的 TEK，AR-RS 可接著提供與移動終端之間的安全通訊，於其中，使用 TEK 來加密資料。

第 9 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 透過請求的金鑰分發來接收 AK。如第 9 圖所示，移動終端 414 傳送信號訊息（例如測距請求 602）至 AR-RS 407，且根據接收金鑰請求 704，基地台 400 證明移動終端 414 之憑據。由於移動終端 414 先前已經歷 IEEE 802.1X 完全認證 206 以獲得 AL 610，因此，對於基地台 400 與移動終端 414 而言，非必要再次經歷此程序。就其本身而論，基地台 400 傳送包括 AK 610 或者包括 TEK 616 之金鑰請求 612 至 AR-RS 407，藉此給予 AR-RS 407 授權且提供與移動終端 414 之安全通訊。接著，AR-RS 407 簡單地執行 MAC 檢查 804，以證明被移動終端 414 所持有的金鑰，藉此證明移動終端 414 之識別。AR-RS 407 接著傳送包括 HMAC 或 CMAC 之測距回應 806 至移動終端 414。

如第 8 圖所討論，假使 AR-RS 407 接收來自基地台 40 之 TEK 616 或接收來自 AR-RS 406 之 TEK 616，AR-RS 407 可跳過 SA-TEK 三方交握程序 214 以及 TEK 三方交握程序 216，藉此改善來自 AR-RS 407 之交遞的效率。

第 10 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移

動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 當前具有對應正交遞之移動終端的 AK。舉例來說，假使移動終端 414 如第 6 圖所示認證 AR-RS 406，離開 AR-RS 406 之覆蓋區域且進入 AR-RS 407 之覆蓋區域，接著返回至 AR-RS 406 之覆蓋區域，AR-RS 406 在其記憶體（例如記憶體 546、ROM 544、RAM 542，或資料庫 548）中仍持有 AK。因此，當移動終端 414 傳送信號訊息時，例如包括對應 AK 610 之認證金鑰識別（AKID）的測距請求 1002，AR-RS 406 傳送 AKID 證明請求 1004 至基地台 400，以證實移動終端 414 之位置。

根據 AKID 證明請求 1004 之接收，基地台 400 證明移動終端 414 之位置。由於移動終端 414 先前已經歷了 IEEE 802.1X 完全認證 203 以獲得 AK 610，因此，對於基地台 400 與移動終端 414 而言，非必要再次經歷此程序。就其本身而論，假使 AR-RS 406 持有 AK 610，基地台 400 傳送包括 AK 610 之金鑰請求 610 至 AR-RS 407，藉此給予 AR-RS 407 授權，以認證且建立與移動終端 414 之間的安全地通訊。假使 AR-RS 406 非持有 AK 610，或者假使 AR-RS 406 需要證實其持有適當的 AK 610，再接收來自基地台 400 之金鑰回應 1006 後，AR-RS 406 可傳送 RNG 回應 606。

根據測距回應 1008 之接收，移動終端 414 可試圖初始化延伸認證協定（EAP）以開始第 7 圖之 IEEE 802.1X 完

全認證。如前所示，由於 AR-RS 407 已以具有 AK 610，AR-RS 407 可傳送延伸認證協定完成訊息至移動終端 414，而不需實際上經歷 IEEE 802.1X 完全認證的程序。

當 AR-RS 407 具有 AK 610 時，其可執行與移動終端 414 之間的 SA-TEK 三方交握程序 214 及 TEK 三方交握程序 216 中之一者或兩者，以準備資料傳送。如第 10 圖所示，在移動終端 120 已被認證後，AR-RS 407 可建立新的 TEK 1010 以將傳送於 AR-RS 407 與移動終端 120 之間的資料加密。如上所述，假使 AR-RS 406 已具有 TEK 616，AR-RS 406 可跳過 SA-TEK 三方交握程序 214 及 TEK 三方交握程序 216，藉此改善來自 AR-RS 407 之交遞之效率，且建立 AR-RS 406 與移動終端 414 之間的安全關聯。

第 11 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 當前具有對應正交遞之移動終端的 AK。在此效率改善之交遞中，當移動終端 414 傳送測距請求 602 時，AR-RS 406 已持有 AK 610，且可簡單地執行 MAC 檢查 804，以證明移動終端 414 所持有的金鑰，且藉此證明移動終端 414 之身份。AR-RS 406 可接著傳送只是 HMAC 或 CMAC 之測距請求 806。

第 12 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 當前具有非對應正交遞之移動終端的 AK。例如，當 AR-RS 408 在其記憶

體（例如記憶體 546、ROM 544、RAM 542，或資料庫 548）中持有 AK 1202(對應除了移動終端 414 以外之移動終端，但不是對應移動終端 414 之 AK 610）時，移動終端 414 可進入 AR-RS 408 之覆蓋範圍。因此，當 AR-RS 407 傳送 AKID 證明請求 1004 至基地台 400 以證實移動終端 414 之位置時，基地台 400 回應對應移動終端 414 之正確 AK，例如 AK 610。

根據測距回應 1008 之接收，移動終端 414 可試圖初始化延伸認證協定（EAP）以開始第 7 圖之 IEEE 802.1X 完全認證。如前所示，由於 AR-RS 408 現在具有 AK 610，AR-RS 408 可傳送延伸認證協定完成訊息至移動終端 414，而不需實際上經歷 IEEE 802.1X 完全認證的程序。

當 AR-RS 408 具有 AK 610 時，其可執行與移動終端 414 之間的 SA-TEK 三方交握程序 214 及 TEK 三方交握程序 216 中之一者或兩者，以準備資料傳送。如第 10 圖所示，在移動終端 120 已被認證後，AR-RS 408 可建立新的資料金鑰（例如 TEK 1204）以加密傳送於 AR-RS 408 與移動終端 120 之間的資料。

第 13 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相同之基地台，且目標 AR-RS 當前具有非對應正交遞之移動終端的 AK。當 AR-RS 414 傳送信號訊息（例如測距請求 602）時，AR-RS 408 持有 AK 1202，以及當 AR-RS 408 執行 MAC 檢查 804 以證明移動終端 414 所持

有的金鑰且藉此證明移動終端 414 之身分時，MAC 檢查不成功。當 AR-RS 408 傳送 AKID 證明請求 1004 至基地台 400 以證實移動終端 414 之位置時，基地台 400 回應適當的 AK，例如 AK 610。AR-RS 408 可接著傳送包括 HMAC 或 CMAC 之測距回應 608。假使 AR-RS 408 以具有 TEK 616，AR-RS 408 可跳過 SA-TEK 三方交握程序 214 及 TEK 三方交握程序 216。

第 7 至 13 圖係說明在連接至相同基地台之當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之例子。雖然前述與第 12 及 13 圖有關的例子係以移動終端（例如 AR-RS 408）為背景來說明，此技術領域之人士可理解第 12 及 13 圖之當前 AR-RS 或目標 AR-RS 可以是固定的中繼站。此技術領域之人士也可理解，在上述關於第 7 至 11 圖中所述每一例子中，當前 AR-RS 或目標 AR-RS 可以是移動中繼站，例如 AR-RS 408。

此技術領域之人士也可理解，在上述關於第 7 至 11 圖中所述每一例子中，以基地台 400 傳送相異安全工具至中繼站，以取代傳送 AK 610 至 AR-RS 406-409。例如，基地台 400 可使用 AK 610 產生證明金鑰（例如 MACK 618）以及資料金鑰（例如 TEK 616），且預先分發證明金鑰及資料金鑰至中繼站 407，以取代傳送 AK 610。

同樣地，根據金鑰請求 704 之接收，基地台 400 此用 AK 610 產生證明金鑰（例如 MACK 618），且在金鑰回應 612 中傳送 MACK 至 AR-RS 407，以做 MAC 檢查 804 之

用。此外，假使 AR-RS 406 在其記憶體（例如記憶體 546、ROM 544、RAM 542，或資料庫 548）中已具有對應移動終端 414 之 MACK 618，根據信號訊息（例如測距請求 602）之接收，AR-RS 406 可執行 MAC 檢查 804。假使中繼站 406 在其記憶體中具有錯誤的 MACK 1206，根據信號訊息（例如測距請求 602）之接收，AR-RS 406 可傳送 AKID 證明請求 1004，並接收來自基地台 400 且在金鑰轉移 1008 中的 MACK 618。

AR-RS 405-408 可使用 MACK 618 來認證或證明移動終端之身分，作為 MAC 之一部分。移動終端 414 及 AR-RS 405-408 可檢查酬載內的 MAC 或 MAC 封包之資料元件，用來認證彼此，或換句話說，用來識別彼此。

第 14 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相異之基地台。初始化程序 1400 用來確保移動終端請求網路服務被授權來存取網路 300，以及提供移動終端與 AR-RS 之間的安全關聯，以允許安全訊息傳送。例如，在移動終端 414 剛由 AR-RS 408 移動進入至由目標 AR-RS 408 所轉遞之目標基地台 1402 所提供之覆蓋區域後，程序 1400 可用來認證且授權移動終端 414。AK 610 當前儲存在移動終端 414，而目標基地台 1402 及目標 AR-RS 2505 則具有儲存在其各自記憶體之 AK 1406。如第 14 圖所示，和正與移動終端 414 交遞之 AR-RS 408 一樣，目標基地台 1402 連接至相同的閘道器，然而，假使目標基

地台 1402 連接至與 AR-RS 408 相異的閘道器，初始化程序 1400 將不會改變。

移動終端 414 傳送包括認證金鑰識別之信號訊息（例如測距請求 1002）至目標 AR-RS 1404，以指示移動終端 414 在目標 AR-RS 1404 之範圍內。目標 AR-RS 1404 傳送包括認證金鑰識別之移動終端認證請求 1407 至目標基地台 1402。目標基地台 1402 接收移動終端認證請求 1407，但由於目標基地台 1402 沒有認可 AK 610，因此其不會證明移動終端 414。因此，目標基地台 1402 可傳送認證失敗回應 1408 至目標 AR-RS 1404，而目標 AR-RS 1404 傳送測距回應 1409 至移動終端 414。目標基地台 1402 可要求移動終端 414 使用 IEEE 802.1X 完全認證協定 206 來認證 AAA 伺服器 104。由於 IEEE 802.1X 完全認證協定 206，因此閘道器 106 將 PMK 1410 分發至移動終端 120。閘道器 106 也透過 AK 傳送（AK Transfer）612 將 AK 1412 傳送至目標基地台 1402。移動終端 414 獨立於 PMK 1410 之外地來計算 AK 610。

在一實施例中，為了允許目標 AR-RS 1404 執行額外認證步驟以提供額外安全給與移動終端連接之網路，基地台 400 傳送包括 AK 1412 之金鑰回應 614 至目標 AR-RS 1404。當目標 AR-RS 1404 具有 AK 1412 時，其執行與移動終端 414 之間的 SA-TEK 三方交握程序 214 及 TEK 三方交握程序 216 中之一者或兩者，以提供進一步安全給與移動終端 414 連接之網路。在 TEK 三方交握程序 216 之

期間，AR-RS 1404 傳送以 KEK 1416 來加密的資料金鑰（例如 TEK 1414）至移動終端 414。TEK 1414 可隨機地由目標 AR-RS 1404 來產生。

第 14 圖係表示在當前 AR-RS 與目標 AR-RS 之間的移動終端交遞之信號示意圖，其中，當前 AR-RS 與目標 AR-RS 連接相異之基地台。此技術領域之人士可瞭解當前 AR-RS 或目標 AR-RS 可以是移動中繼站，例如 AR-RS 408。

此技術領域之人士也可瞭解，在第 14 圖之相關例子中，基地台 400 可傳送相異安全工具至中繼站 406-409，以取代傳送 AK 610 至 AR-RS 406-409。例如，根據 AK 17412 之接收，基地台 1402 可使用 AK 610 來產生證明金鑰，例如 MACK 618，且傳送證明金鑰至 AR-RS 1404，以取代傳送 AK 1412。

雖然前述關於初始化及交遞之程序應用在移動中繼站，但移動中繼站以及存取來自移動中繼站內之網路的移動終端，也必須為了基地台內的改變而準備，於其中 AR-RS（特別是移動中繼站）不會改變。

第 15 圖係表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖。在第 15 圖中，當 AR-RS 408 移動或即將移動至目標基地台 1502 之覆蓋區域時，移動中繼站 AR-RS 408 與目標基地台 1502 關聯。移動終端 416 及 418 連接 AR-RS 408，且在轉變至目標基地台 1502 之期間，最好維持與 AR-RS 408 之連接。為了更新移動終端 416 及 418 之 AK，AR-RS 408 可發佈範圍訊息 1504 至目標基

地台 1502，其對基地台 1502 指示出 AR-RS 408 在處於或接近於目標基地台 1502 之覆蓋區域內。根據範圍訊息 1504 之接收，AR-RS 408 接受與閘道器 106 與 AAA 伺服器 104 之間的 IEEE 802.1X 完全認證協定 206、SA-TEK 三方交握程序 214、及 TEK 三方交握程序 216 中之一者或多個。就其本身而論，AR-RS 408 必須接收 AK 且必須以與移動終端相似的方法來被認證。閘道器 106 可在 AK 傳送 1506 中將 AK 傳送給移動中繼站。

AR-RS 408 傳送再次認證觸發訊息 1508 至移動終端 416 及 418。根據再次認證觸發訊息 1508 之接收，移動終端 416 及 418 執行與閘道器 106 與 AAA 伺服器 104 之間的 IEEE 802.1X 完全認證協定 206。閘道器 106 計算由閘道器中現存 PMK 所獲得的新 AK 給目標基地台 1502。閘道器 106 在 AK 傳送 1510 中，轉移所有的 AK 給與 AR-RS 408 關聯之移動終端，且可在一隧道模式下執行，於其中，與 AR-RS 408 連接之所有移動終端之所有參數（例如 AK）一次被傳送。在隧道模式下，在兩節點之間的邏輯連接是專用的，例如 AR-RS 408 與閘道器 106 之間，且中間節點（例如目標基地台 1502）無法處理此通道封包，但只遞送通道封包。移動終端 416 至 418 接著接受與目標基地台 1502 之間的 SA-TEK 三方交握程序 214。目標基地台 1502 在 TEK 轉移 1512 中將提供每一移動終端之資料金鑰及 AK 給 AR-RS 408，且使用隧道模式來執行。在一實施例中，在中間基地台交遞之前，AK 在基地台 1502 及移動終端 416

及 418 上被接收，以避免對移動終端 416 及 418 之服務中斷。

此技術領域之人士可瞭解，雖然第 15 圖表示透過閘道器 106 與網路及 AAA 伺服器 104 通訊之目標基地台 1502，但目標基地台 1502 也可透過閘道器 108 或其他閘道器，以第 15 圖所述之相同程序來與網路及 AAA 伺服器 104 通訊。

第 16 圖係表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖，其中，目標基地台 1600 與相異的閘道器（例如閘道器 1602）通訊，且 AR-RS 408 可接收 AK 且作為移動終端 416 及 418 之證明者。為了更新移動終端 416 及 418 之 AK，AR-RS 408 可發佈範圍訊息 1504 至目標基地台 1600，其向基地台 1600 指示 AR-RS 408 處於或接近於目標基地台 1600 之覆蓋區域。在 AR-RS 408 接收與閘道器 1602 之間的 IEEE 802.1X 完全認證協定 206 後，閘道器 1602 在 AK 轉移 1606 中轉移 AK 給移動中繼站。AR-RS 408 也接受 SA-TEK 三方交握程序 214，以獲得關於通道封包之進一步資料傳送的資料金鑰，或者轉遞移動終端訊息。

AR-RS 408 傳送再次認證觸發訊息 1508 至移動終端 416 及 418。根據再次認證觸發訊息 1508 之接收，移動終端 416 及 418 執行與閘道器 1602 與 AAA 伺服器 104 之間的 IEEE 802.1X 完全認證協定 206。閘道器 1602 計算新 AK 給移動終端 416 及 418 中每一者，且在 AK 傳送 1608 中轉移所有的 AK 給與 AR-RS 408 相關聯之移動終端。在一實

施例中，AR-RS 408 如一個 AR-RS 般操作，且具有直接認證移動終端之能力。在隧道模式下，閘道器 1602 傳送對應移動終端 416 及 418 之 AK。移動終端 416 及 418 接著接收與 AR-RS 408 之間的 SA-TEK 三方交握程序 214。AR-RS 408 使用 SA-TEK 三方交握程序轉移，將提供每一移動終端之資料金鑰給 AR-RS 408。二者擇一地，假使 AR-RS 408 接收來自另一 AR-RS 或來自目標基地台 1602 之資料金鑰，AR-RS 408 在操作上可避免產生移動終端 416 及 418 之新資料金鑰。

第 17 圖係表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖，其中，基地台連接至相同閘道器。在第 17 圖中，AR-RS 408 由基地台 1502（第 15 圖）之覆蓋區域已移動或將移動至目標基地台 1702 之覆蓋區域。目標基地台 1702 及當前基地台 1502 由相同的閘道器 106 所服務。AR-RS 408 發佈範圍訊息 1504 至目標基地台 1702，其對目標基地台 1702 指示 AR-RS 408 處於或接近於目標基地台 1702 之覆蓋區域。AR-RS 408 透過閘道器 106 來認證且執行認證協定，例如 SA-TEK 三方交握程序 214。在 AR-RS 408 被認證後，閘道器 106 在 AK 傳送 1706 中傳送移動終端 416 及 418 之 AK 至 AR-RS 408。當多個 AK 由閘道器 106 傳送至 AR-RS 408 時，閘道器 106 可在 AK 傳送 1706 中以隧道模式來傳送 AK。AR-RS 408 傳送再次認證觸發訊息 1508 至移動終端 416 及 418。根據再次認證觸發訊息 1508 之接收，移動終端 416 及 418 執行與

AR-RS 408之間的SA-TEK 三方交握程序214，以更新其各自的 AK，且執行使程序時也可以或不需同時更新其各自的資料金鑰。在一實施例中，在中間基地台交遞之前，AK在AR-RS 408上被接收，以避免對移動終端416及418之服務中斷。

第 18 圖係表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖，其中，基地台連接至相同閘道器。在第18圖中，AR-RS 408由基地台1502之覆蓋區域已移動或將移動至目標基地台 1702 之覆蓋區域。AR-RS 408發佈範圍訊息1504至目標基地台1702，其對目標基地台1702指示AR-RS 408處於或接近於目標基地台1702之覆蓋區域。根據範圍訊息之接收，目標基地台1702傳送移動終端416及418之每一者的AK給AR-RS 408。此程序是可允許的，是因為由於在閘道器106內基地台1502之先前的認證，基地台 1702 必須存取移動終端 416 及 418 之AK。當多個AK由目標基地台1502傳送至AR-RS 408時，目標基地台1502可在AK傳送1802中以隧道模式來傳送AK。AR-RS 408傳送再次認證觸發訊息1508至移動終端416及418。根據再次認證觸發訊息1508之接收，移動終端416及418執行與AR-RS 408之間的SA-TEK 三方交握程序214，以更新其各自的AK，且執行使程序時也可以或不需同時更新其各自的資料金鑰。在一實施例中，在中間基地台交遞之前，AK在AR-RS 408上被接收，以避免對移動終端416及418之服務中斷。

此技術領域之人士可瞭解，在第 15-18 圖中所述之例子，取代傳送 AK 至目標基地台 1502，閘道器 106 可傳送不同之安全工具至移動終端，例如對應 AR-RS 408 之證明金鑰。同樣地，取代將移動終端 416 及 418 之 AK 傳送至 AR-RS 408，目標基地台 1502 可傳送相異的安全工具，例如對應移動終端 416 及 418 之證明金鑰。

在此揭露之系統及方法可實施在數位電子電路或在電腦硬體、韌體、軟體、或其結合。利用本發明之裝置可實施在電腦程式產品，此電腦程式產品包含在關於可程式化處理器所執行的機械可讀取儲存裝置。包含本發明之方法步驟可由可程式化處理器來執行，其實行指令程式，以藉由根據輸入資料之操作及產生輸出信號來執行本發明之功能。包含本發明之實施例可實施在可程式化系統中可執行的一或多個電腦程式，其包括用來接收來自儲存系統之資料以及傳送資料至儲存系統之至少一個可程式化處理器、至少一個輸入裝置、以及至少一個輸出裝置。電腦程式可實施在高階或物件導向程式語言、以及/或組合或機械編碼。語言或編碼可以示編譯或翻譯語言或編碼。處理器可包括一般或特別木訂微處理器。處理器接收來自記憶體之指令或資料。包含電腦程式指令和資料之儲存裝置包括所有型態的非揮發記憶體，包括半導體記憶裝置，例如 EPROM、EEPROM、以及快閃記憶裝置；磁碟機，例如內部硬碟及卸除式硬碟；以及 CD-ROM。上述的任一種可由 ASIC 來補充或包含在 ASIC 內。

此技術領域之人士可知，不同的修改和變化可應用於在無線通訊系統中建立安全關聯之系統及方法。例如，此技術領域之人士可瞭解測距請求和回應是一種信號訊息類型，且其他信號訊息可被使用。此外，此技術領域之人士可瞭解，流量編碼金鑰是一種資料金鑰的類型，而其他資料金鑰可被使用，且 MACK 是一種認證金鑰的類型，而其他認證金鑰可被使用。此技術領域之人士也可瞭解，基地台與中繼站之間可以是無線通訊或有線通訊。本發明雖以較佳實施例揭露如上，然其並非用以限定本發明的範圍，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可做些許的更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

第 1 圖表示使用 IEEE 802.16d/802.16e WiMAX 無線通信系統的一習知無線通信系統的方塊圖；

第 2 圖表示 IEEE 802.16d/802.16e WiMAX 無線通信系統中習知的認證與授權運作的信號流程圖；

第 3 圖表示為使用 IEEE 802.16j WiMAX 且具有多節點跳躍中繼網路協定技術架構的通信系統的一習知通信系統的方塊圖；

第 4 圖表示根據本發明之使用在 IEEE 802.16j WiMAX 無線通信系統的一無線通信系統的一實施例的方塊圖，其中該無線通信系統選擇使用中繼站作為認證中繼站；

第 5A 圖表示一基地台的一實施例的方塊示意圖；

第 5B 圖表示一移動終端的一實施例的方塊示意圖；

第 5C 圖表示中繼站或移動中繼站的一實施例的方塊示意圖；

第 6 圖表示在 IEEE 802.16j WiMAX 無線通訊系統中認證及授權之信號示意圖，於此無線通訊系統中，被選擇之中繼站作為認證中繼站；

第 7 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與目標認證中繼站連接相同之基地台，且目標認證中繼站當前不持有要求的認證金鑰；

第 8 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與

目標認證中繼站連接相同之基地台，且目標認證中繼站透過未經請求的金鑰預先分發來接收指示；

第 9 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與目標認證中繼站連接相同之基地台，且目標認證中繼站透過請求的金鑰分發來接收認證金鑰；

第 10 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與目標認證中繼站連接相同之基地台，且目標認證中繼站當前具有對應正交遞之移動終端的認證金鑰；

第 11 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與目標認證中繼站連接相同之基地台，且目標認證中繼站當前具有對應正交遞之移動終端的認證金鑰；

第 12 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與目標認證中繼站連接相同之基地台，且目標認證中繼站當前具有非對應正交遞之移動終端的認證金鑰；

第 13 圖係表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站與目標認證中繼站連接相同之基地台，且目標認證中繼站當前具有非對應正交遞之移動終端的認證金鑰；

第 14 圖表示在當前認證中繼站與目標認證中繼站之間的移動終端交遞之信號示意圖，其中，當前認證中繼站

與目標認證中繼站連接相異之基地台；

第 15 圖表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖；

第 16 圖表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖，其中，目標基地台 1600 與相異的閘道器通訊，且認證中繼站 408 可接收 AK 且作為移動終端 416 及 418 之證明者；

第 17 圖表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖，其中，基地台連接至相同閘道器；

第 18 圖表示在當前基地台與目標基地台之間移動中繼站交遞之信號示意圖，其中，基地台連接至相同閘道器。

【主要元件符號說明】

100～網路；

102～連線服務網路；

104～AAA 伺服器；

106、108～閘道器；

110-115～基地台；

120、122、124～移動終端；

126、128～用戶終端；

200～初始化程序；

202～測距請求；

204～測距回應；

206～IEEE 802.1X 完整認證程序；

208～主會談金鑰（MSK）；

210～對稱主金鑰(PMK)；

212～認證金鑰（AK）；

214～SA-TEK 三方交握程序；

215～訊息認證編碼金鑰（MACK）；

216～TEK 三方交錯程序；

218～金鑰加密金鑰（KEK）；

220～資料加密金鑰（TEK）；

300～核心網路；

310-313～基地台；

320、322、324、326～移動終端；

328、330、332～中繼站；

334～移動中繼站；

400～基地台；

402、404～中繼站；

406、407、408、409～認證中繼站；

410～中繼金鑰；

412～安全中繼區；

414、416、418～移動終端；

500、520、540～中央處理單元（CPU）；

502、522、542～隨機存取記憶體（RAM）；

504、524、544～隨機唯讀記憶體（ROM）；

506、526、546～記憶體；

508、528、548～資料庫；

510、530、550～輸入/輸出（I/O）裝置；

512、532、552～介面；

514、534、554～天線；

600～初始化程序；

602～測距請求；

604～移動終端認證請求；

606～測距回應；

608～對稱主金鑰(PMK)；

610～認證金鑰（AK）；

612～AK 傳送（金鑰請求及回應）；

614～金鑰回應；

616～資料加密金鑰（TEK）；

618～訊息認證編碼金鑰（MACK）；

708～起使請求；

710～PKMv2-EAP 完整訊息；

712～～資料加密金鑰（TEK）；

802～金鑰預先分發信號；

804～訊息認證編碼（MAC）檢查；

806～測距回應；

1002～測距請求；

1004～認證金鑰識別（AKID）證明請求；

1006～金鑰回應；

1010～資料加密金鑰（TEK）；

1008～測距回應；

1202～認證金鑰（AK）；

1204～資料加密金鑰（TEK）；

1206～訊息認證編碼金鑰（MACK）；

1402～基地台；

1404～認證中繼站；

1406～認證金鑰（AK）；

1407～移動終端認證請求；

1408～認證失敗回應；

1409～測距回應；

1410～對稱主金鑰(PMK)；

1412～認證金鑰（AK）；

1414～資料加密金鑰（TEK）；

1416～金鑰加密金鑰（KEK）；

1502～基地台；

1504～範圍訊息；

1506～認證金鑰（AK）轉移；

1508～再次認證觸發訊息；

1510～認證金鑰（AK）轉移；

1512～資料加密金鑰（TEK）/認證金鑰（AK）轉移；

1600～基地台；

1602～閘道器；

1606、1608～認證金鑰（AK）轉移；

1702～基地台；

1706～認證金鑰（AK）轉移；

1802～認證金鑰（AK）轉移。

## 十、申請專利範圍：

1.一種提供安全通訊之方法，適用於在一通訊網路上之一基地台、一中繼站、以及一移動終端之間，該方法包括：

由該中繼站接收來自該基地台未經請求之一安全金鑰；

由該中繼站接收來自該移動終端之一信號訊息；以及

由該中繼站使用該安全金鑰來認證該移動終端，其中來自該基地台之未經請求之該安全金鑰係由一預先認證產生。

2.如申請專利範圍第 1 項所述之提供安全通訊之方法，接收該信號訊息之該步驟包括接收一測距請求。

3.如申請專利範圍第 1 項所述之提供安全通訊之方法，更包括接收該安全金鑰作為一主要金鑰（master key）。

4.如申請專利範圍第 3 項所述之提供安全通訊之方法，更包括接收該主要金鑰作為一認證金鑰（authentication key，AK）。

5.如申請專利範圍第 1 項所述之提供安全通訊之方法，更包括接收該安全金鑰作為一證明金鑰（verification key）。

6.如申請專利範圍第 5 項所述之提供安全通訊之方法，其中，接收該安全金鑰作為該證明金鑰之該步驟包括接收該安全金鑰作為一訊息認證編碼金鑰（message authentication code key，MACK）。

7.如申請專利範圍第 1 項所述之提供安全通訊之方法，更包括接收包括對應該移動終端之一訊息認證編碼（message authentication code，MAC）的該信號訊息，其中，認證該移動終端之該步驟包括使用該安全金鑰來證明該訊息認證編碼。

8.如申請專利範圍第 1 項所述之提供安全通訊之方法，更包括由該中繼站來執行與該移動終端之間的一安全關聯信號協定以及一資料加密金鑰三方交握程序（TEK 3-Way handshake procedure）中至少一者。

9.如申請專利範圍第 8 項所述之提供安全通訊之方法，其中，由該中繼站來執行與該移動終端之間的該安全關聯信號協定以及該資料加密金鑰三方交握程序中至少一者之該步驟包括，執行與該移動終端之間的一安全關聯與資料加密金鑰三方交握程序（Security Association and Traffic Encryption Key (SA-TEK) 3-Way handshake procedure）與該資料加密金鑰三方交握程序中至少一者。

10.如申請專利範圍第 1 項所述之提供安全通訊之方法，更包括：

由該中繼站產生一資料金鑰；以及

由該中繼站使用該資料金鑰來傳送一加密資料至該移動終端。

11.如申請專利範圍第 1 項所述之提供安全通訊之方法，更包括由該中繼站來執行移動至一相異基地台之一服務區域。

12.如申請專利範圍第 1 項所述之提供安全通訊之方法，其中，該基地台與該中繼站之間為無線通訊。

13.一種提供安全通訊之方法，適用於在一通訊網路上之一基地台、一中繼站、以及一移動終端之間，該方法包括：

由該中繼站接收來自該移動終端之一信號訊息；

在接收該信號訊息之後，由該中繼站傳送一安全金鑰請求至該基地台；

根據先前傳送之該安全金鑰請求，由該中繼站接收來自該基地台之一安全金鑰；以及

由該中繼站使用接收之該安全金鑰來認證該移動終端。

14.如申請專利範圍第 13 項所述之提供安全通訊之方法，其中，接收該信號訊息之該步驟包括接收一測距請求。

15.如申請專利範圍第 13 項所述之提供安全通訊之方法，更包括接收該安全金鑰作為一主要金鑰(master key)。

16.如申請專利範圍第 15 項所述之提供安全通訊之方法，更包括接收該主要金鑰作為一認證金鑰(authentication key，AK)。

17.如申請專利範圍第 13 項所述之提供安全通訊之方法，更包括接收該安全金鑰作為一證明金鑰(verification key)。

18.如申請專利範圍第 17 項所述之提供安全通訊之方法，其中，接收該安全金鑰作為該證明金鑰之該步驟包括

接收該安全金鑰作為一訊息認證編碼金鑰（message authentication code key，MACK）。

19.如申請專利範圍第 13 項所述之提供安全通訊之方法，更包括接收包括對應該移動終端之一訊息認證編碼（message authentication code，MAC）的該信號訊息，其中，認證該移動終端之該步驟包括使用該安全金鑰來證明該訊息認證編碼。

20.如申請專利範圍第 13 項所述之提供安全通訊之方法，更包括由該中繼站來執行與該移動終端之間的一安全關聯信號協定以及一資料加密金鑰三方交握程序（TEK 3-Way handshake procedure）中至少一者。

21.如申請專利範圍第 20 項所述之提供安全通訊之方法，其中，由該中繼站來執行與該移動終端之間的該安全關聯信號協定以及該資料加密金鑰三方交握程序中至少一者之該步驟包括，執行與該移動終端之間的一安全關聯與資料加密金鑰三方交握程序（Security Association and Traffic Encryption Key (SA-TEK) 3-Way handshake procedure）與該資料加密金鑰三方交握程序中至少一者。

22.如申請專利範圍第 13 項所述之提供安全通訊之方法，更包括：

由該中繼站產生一資料金鑰；以及

由該中繼站使用該資料金鑰來傳送一加密資料至該移動終端。

23.如申請專利範圍第 13 項所述之提供安全通訊之方

法，更包括由該中繼站來執行移動至一相異基地台之一服務區域。

24.如申請專利範圍第 13 項所述之提供安全通訊之方法，其中，該基地台與該中繼站之間為無線通訊。

25.一種提供安全通訊之方法，適用於在一通訊網路上之一目標基地台、一移動中繼站、以及至少一移動終端之間，該方法包括：

由該移動中繼站傳送一信號訊息至該目標基地台，其中，該信號訊息包括對應該至少一移動終端之一訊息認證編碼（message authentication code，MAC）；

由該移動終端接收來自該目標基地台之一回應信號訊息；

由該移動中繼站接收來自該目標基地台且對應該至少一移動終端之至少一安全金鑰；以及

由該移動中繼站使用對應之該安全金鑰來認證該至少一移動終端。

26.如申請專利範圍第 25 項所述之提供安全通訊之方法，其中，接收對應該至少一移動終端之該至少一安全金鑰之該步驟包括在一安全隧道模式下接收該至少一安全金鑰。

27.如申請專利範圍第 25 項所述之提供安全通訊之方法，其中，認證該至少一移動終端之該步驟包括執行 IEEE 802.1X 認證。

28.如申請專利範圍第 25 項所述之提供安全通訊之方

法，更包括在該移動中繼站與該目標基地台之間執行一安全關聯信號協定以及一資料加密金鑰三方交握程序（TEK 3-Way handshake procedure）中至少一者。

29.如申請專利範圍第 28 項所述之提供安全通訊之方法，其中，由該移動中繼站在該移動中繼站與該目標基地台之間執行該安全關聯信號協定以及該資料加密金鑰三方交握程序中至少一者之步驟包括，執行與該移動終端之間的一安全關聯與資料加密金鑰三方交握程序（Security Association and Traffic Encryption Key (SA-TEK) 3-Way handshake procedure)與該資料加密金鑰三方交握程序中至少一者。

30.如申請專利範圍第 25 項所述之提供安全通訊之方法，其中，接收該至少一安全金鑰之該步驟包括在一隧道模式下接收該至少一安全金鑰。

31.如申請專利範圍第 25 項所述之提供安全通訊之方法，接收該至少一安全金鑰之該步驟包括接收一認證金鑰（authentication key，AK）。

32.如申請專利範圍第 25 項所述之提供安全通訊之方法，更包括接收該安全金鑰作為一證明金鑰（verification key）。

33.如申請專利範圍第 32 項所述之提供安全通訊之方法，其中，接收該安全金鑰作為該證明金鑰之該步驟包括接收該安全金鑰作為訊息認證編碼金鑰（message authentication code key，MACK）。

34.如申請專利範圍第 25 項所述之提供安全通訊之方法，其中，該目標基地台與該移動中繼站之間為無線通訊。

35 一種中繼站，用以在一通訊網路上提供安全通訊，該中繼站包括：

至少一記憶體，用以儲存複數資料及複數指令；以及

至少一處理器，用以存取該記憶體，其中，當該處理器執行該等指令時，該處理器根據接收自一移動終端之一信號訊息，使用接收自一基地台之未經請求之一安全金鑰來認證該移動終端，其中來自該基地台之未經請求之該安全金鑰係由一預先認證產生。

36.如申請專利範圍第 35 項所述之中繼站，其中，該信號訊息為一測距請求。

37.如申請專利範圍第 35 項所述之中繼站，其中，該安全金鑰為一主要金鑰（master key）。

38.如申請專利範圍第 37 項所述之中繼站，其中，該主要金鑰為一認證金鑰（authentication key，AK）。

39.如申請專利範圍第 35 項所述之中繼站，其中，該安全金鑰為一證明金鑰（verification key）。

40.如申請專利範圍第 39 項所述之中繼站，其中，該證明金鑰為一訊息認證編碼金鑰（message authentication code key，MACK）。

41.如申請專利範圍第 35 項所述之中繼站，其中，該信號訊息包括對應該移動終端之一訊息認證編碼（message authentication code，MAC），且該處理器使用該安全金鑰

來證明該訊息認證編碼。

42.如申請專利範圍第 35 項所述之中繼站，其中，當該處理器執行該等指令時，該處理器更執行與該移動終端之間的一安全關聯信號協定以及一資料加密金鑰三方交握程序（TEK 3-Way handshake procedure）中至少一者。

43.如申請專利範圍第 42 項所述之中繼站，其中，該安全關聯信號協定為一安全關聯與資料加密金鑰三方交握程序（Security Association and Traffic Encryption Key (SA-TEK) 3-Way handshake procedure）。

44.如申請專利範圍第 35 項所述之中繼站，其中，當該處理器執行該等指令時，該處理器產生一資料金鑰，且使用該資料金鑰來傳送一加密資料至該移動終端。

45.如申請專利範圍第 35 項所述之中繼站，其中，該中繼站為一移動中繼站。

46.如申請專利範圍第 35 項所述之中繼站，其中，該基地台與該中繼站之間為無線通訊。

47.一種中繼站，用以在一通訊網路上提供安全通訊，該中繼站包括：

至少一記憶體，用以儲存複數資料及複數指令；以及

至少一處理器，用以存取該記憶體；

其中，當該處理器執行該等指令時，該處理器在接收來自一移動終端之一信號訊息之後，傳送一安全金鑰請求至一基地台，且根據先前傳送之該安全金鑰請求，使用來自該基地台之該安全金鑰來認證該移動終端。

48.如申請專利範圍第 47 項所述之中繼站，其中，該信號訊息為一測距請求。

49.如申請專利範圍第 47 項所述之中繼站，其中，該安全金鑰為一主要金鑰（master key）。

50.如申請專利範圍第 49 項所述之中繼站，其中，該主要金鑰為一認證金鑰（authentication key，AK）。

51.如申請專利範圍第 47 項所述之中繼站，其中，該安全金鑰為一證明金鑰（verification key）。

52.如申請專利範圍第 51 項所述之中繼站，其中，該證明金鑰為一訊息認證編碼金鑰（message authentication code key，MACK）。

53.如申請專利範圍第 47 項所述之中繼站，其中，該信號訊息包括一訊息認證編碼（message authentication code，MAC），且該處理器使用該安全金鑰來證明該訊息認證編碼。

54.如申請專利範圍第 47 項所述之中繼站，其中，當該處理器執行該等指令時，該處理器更執行與該移動終端之間的一安全關聯信號協定以及一資料加密金鑰三方交握程序（TEK 3-Way handshake procedure）中至少一者。

55.如申請專利範圍第 54 項所述之中繼站，其中，該安全關聯信號協定為一安全關聯與資料加密金鑰三方交握程序（Security Association and Traffic Encryption Key (SA-TEK) 3-Way handshake procedure）。

56.如申請專利範圍第 47 項所述之中繼站，其中，當

該處理器執行該等指令時，該處理器產生一資料金鑰，且使用該資料金鑰來傳送一加密資料至該移動終端。

57.如申請專利範圍第 47 項所述之中繼站，其中，該中繼站為一移動中繼站。

58.如申請專利範圍第 47 項所述之中繼站，其中，該基地台與該中繼站之間為無線通訊。

59.一種基地台，用以在一通訊網路上提供安全通訊，該基地台包括：

至少一記憶體，用以儲存複數資料及複數指令；以及

至少一處理器，用以存取該記憶體；

其中，當該處理器執行該等指令當，根據一移動終端進入至一基地台之一覆蓋區域內的指示，該處理器將接收自一認證、授權、及記錄伺服器之未經請求之一主要金鑰。傳送至一中繼站，其中來自該基地台之未經請求之該主要金鑰係由一預先認證產生。

60.如申請專利範圍第 59 項所述之基地台，其中，該未經請求之主要金鑰為一認證金鑰（authentication key，AK）。

61.如申請專利範圍第 59 項所述之基地台，其中，該基地台與該中繼站之間為無線通訊。

62.一種基地台，用以在一通訊網路上提供安全通訊，該基地台包括：

至少一記憶體，用以儲存複數資料及複數指令；以及

至少一處理器，用以存取該記憶體；

其中，當該處理器執行該等指令時，根據接收自一中繼站之一安全金鑰，該處理器將一安全金鑰傳送至一中繼站。

63.如申請專利範圍第 61 項所述之基地台，其中，該基地台與該中繼站之間為無線通訊。

64.一種提供安全通訊之系統，包括：

一基地台，用以提供對一通訊網路之存取、認證在該通訊網路上之一移動終端、接收至少一安全金鑰、以及預先分發該至少一安全金鑰；以及

一中繼站，與該基地台通訊，用以接收預先分發之該至少一未經授權之安全金鑰，且使用該安全金鑰來提供安全資料傳送至該認證之移動終端；

其中，該安全金鑰包括一主要金鑰（master key），以及其中來自該基地台之未經授權之該安全金鑰係由一預先認證產生。

65.如申請專利範圍第 64 項所述之系統，其中，該主要金鑰為一認證金鑰（authentication key，AK）。

66.如申請專利範圍第 64 項所述之系統，其中，該安全金鑰為一訊息認證編碼金鑰（message authentication code key，MACK）。

67.如申請專利範圍第 64 項所述之系統，其中，該基地台與該中繼站之間為無線通訊。

68.一種提供安全通訊之系統，包括：

一基地台，用以提供對一通訊網路之存取、認證在該

通訊網路上之一移動終端、接收至少一安全金鑰、接收至少一安全金鑰請求、以及根據該安全金鑰請求來傳送該至少一安全金鑰；以及

一中繼站，與該基地台通訊，用以傳送該至少一安全金鑰請求至該基地台、根據該安全金鑰請求接收來自該基地台之該至少一安全金鑰、以及使用該安全金鑰提供安全資料傳送至一移動終端；

其中，該安全金鑰包括一認證金鑰（authentication key，AK）及一證明金鑰（verification key）中至少一者。

69.如申請專利範圍第 68 項所述之系統，其中，該證明金鑰為一訊息認證編碼金鑰（message authentication code key，MACK）。

70.如申請專利範圍第 68 項所述之系統，其中，該基地台與該中繼站之間為無線通訊。

71.一種提供安全通訊之方法，適用於在一通訊網路上之一基地台、一中繼站、以及一移動終端之間，該方法包括：

根據來自該中繼站之一金鑰請求的接收，執行一金鑰分發，以將對應該移動終端之一證明金鑰分發至該中繼站；以及

由該中繼站執行一金鑰證明，以識別該移動終端。

72.如申請專利範圍第 71 項所述之提供安全通訊之方法，其中，執行該金鑰分發之步驟包括分發一訊息認證編碼金鑰（message authentication code key，MACK）。

73.如申請專利範圍第 71 項所述之提供安全通訊之方法，更包括由該移動終端執行一金鑰證明，以識別該中繼站。

74.如申請專利範圍第 71 項所述之提供安全通訊之方法，其中，該基地台與該中繼站之間為無線通訊。

75.一種提供安全通訊之方法，適用於在一通訊網路上之一基地台、一中繼站、以及一移動終端之間，該方法包括：

執行一金鑰預先分發，以將對應該移動終端之一未經請求之證明金鑰分發至該中繼站；以及

由該中繼站執行一金鑰證明，以識別該移動終端，其中來自該基地台之未經請求之該證明金鑰係由一預先認證產生。

76.如申請專利範圍第 75 項所述之提供安全通訊之方法，其中，執行該金鑰分發之步驟包括分發一訊息認證編碼金鑰（message authentication code key，MACK）。

77.如申請專利範圍第 75 項所述之提供安全通訊之方法，更包括由該移動終端執行一金鑰證明，以識別該中繼站。

78.如申請專利範圍第 75 項所述之提供安全通訊之方法，其中，該基地台與該中繼站之間為無線通訊。

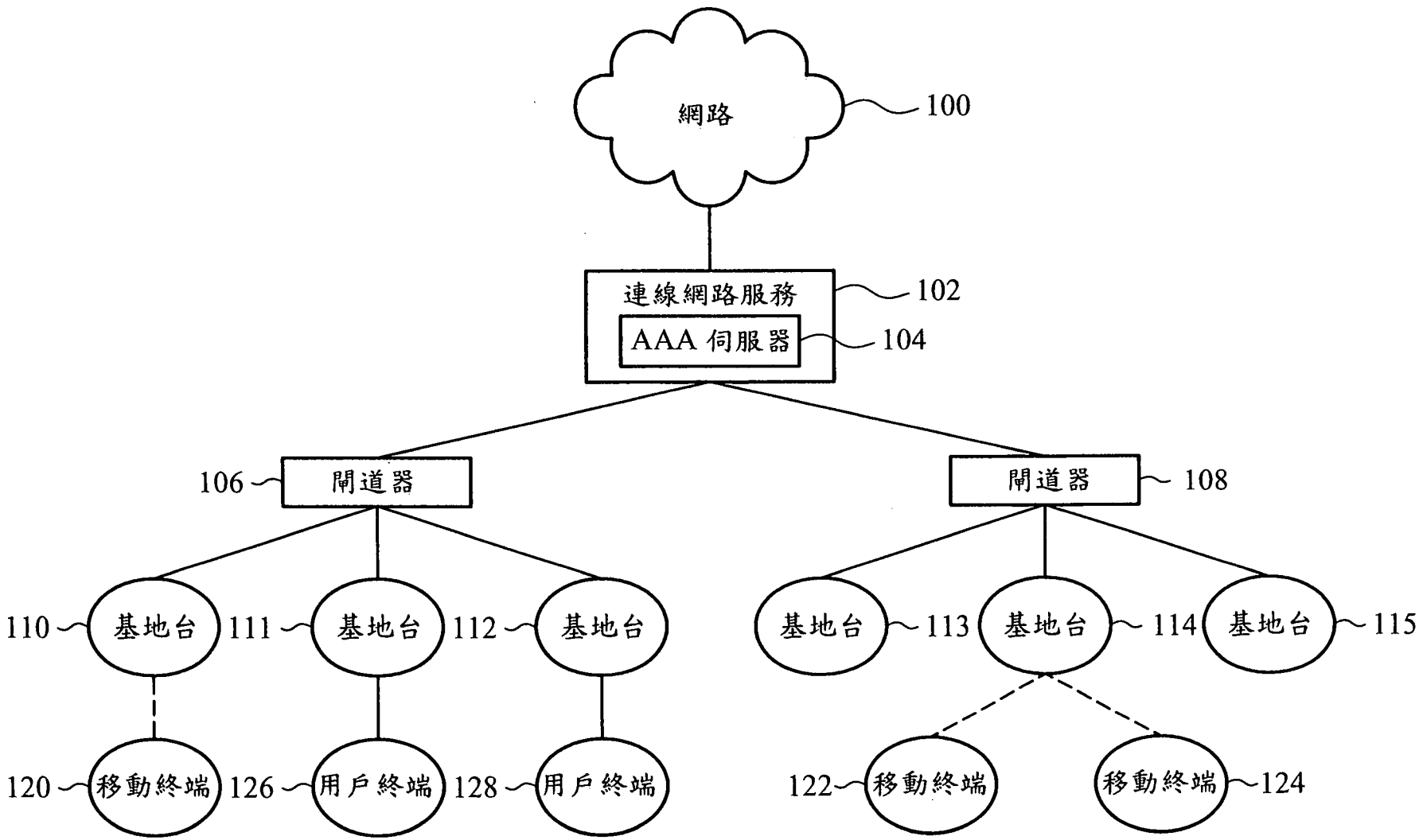
79.一種提供安全通訊之方法，適用於在一通訊網路上之一基地台、一中繼站、以及一移動終端之間，該方法包括：

由該中繼站執行金鑰證明，以識別該移動終端；以及由該移動終端執行金鑰證明，以識別該中繼站。

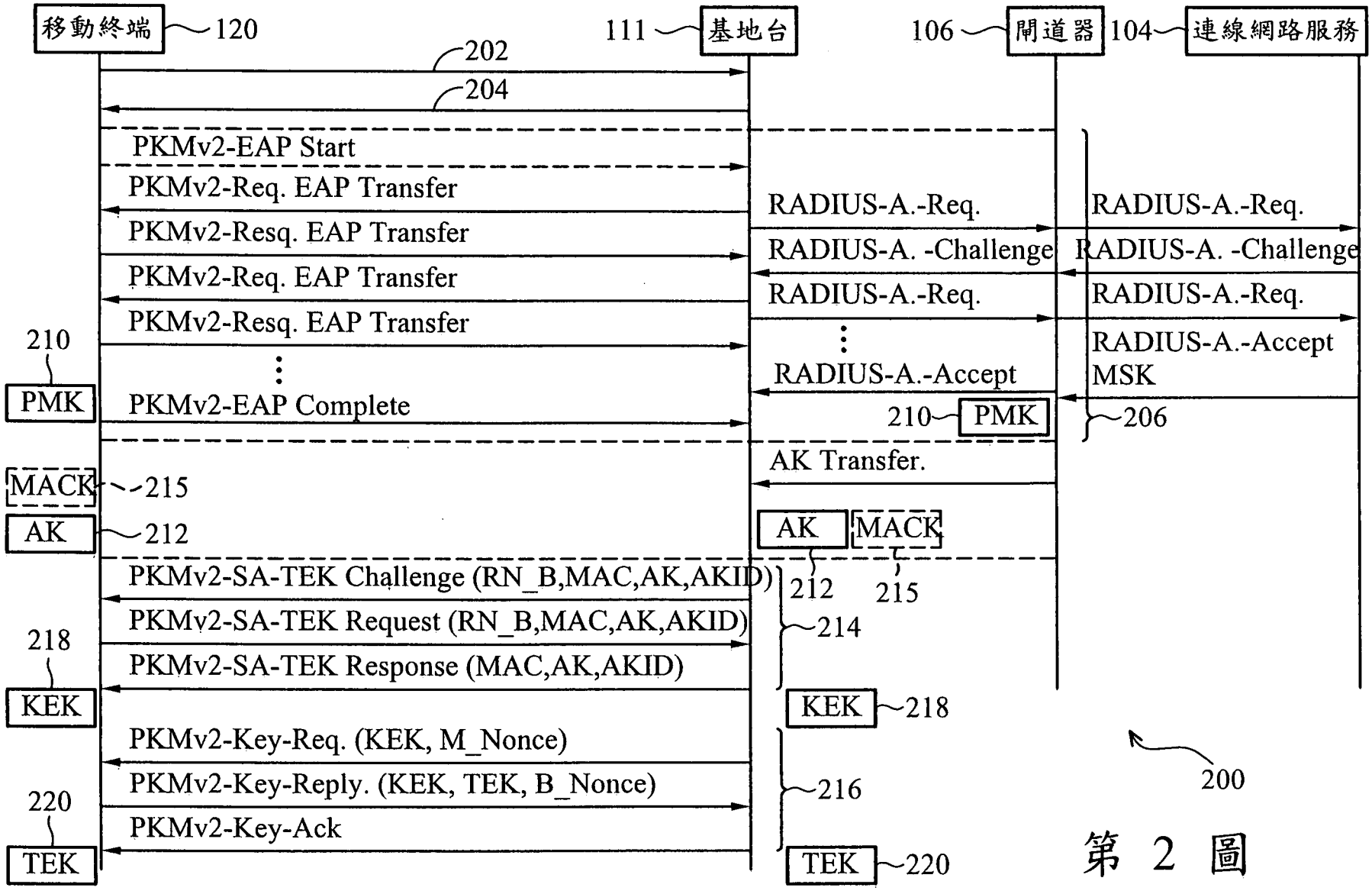
80.如申請專利範圍第 79 項所述之提供安全通訊之方法，其中，該基地台與該中繼站之間為無線通訊。

103年1月23日修正替換頁

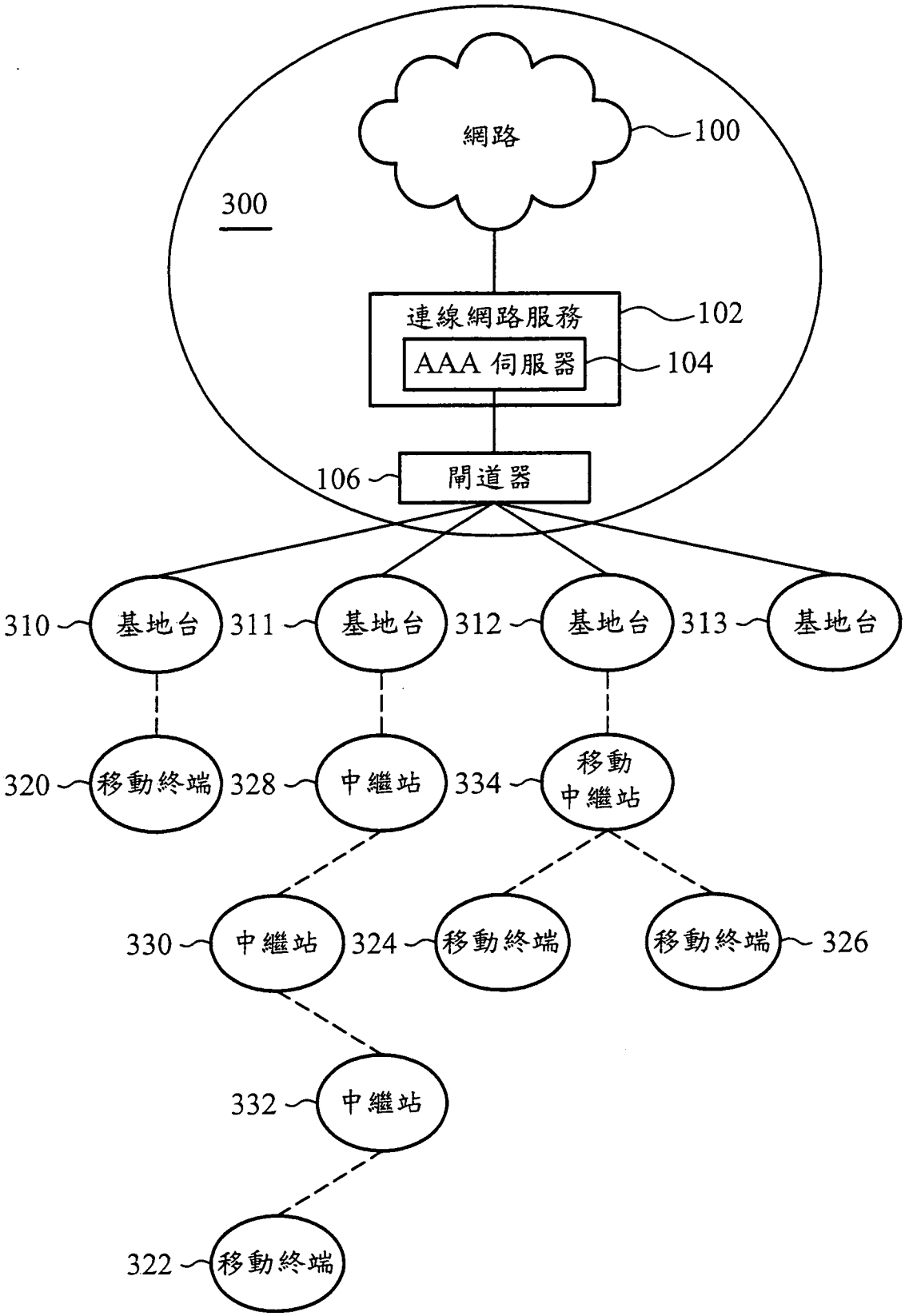
十一、圖式：


網路
100
連線網路服務
102
AAA 伺服器
104
106
閘道器
108
閘道器
110
基地台
111
基地台
112
基地台
113
基地台
114
基地台
115
120
移動終端
126
用戶終端
128
用戶終端
122
移動終端
移動終端
124

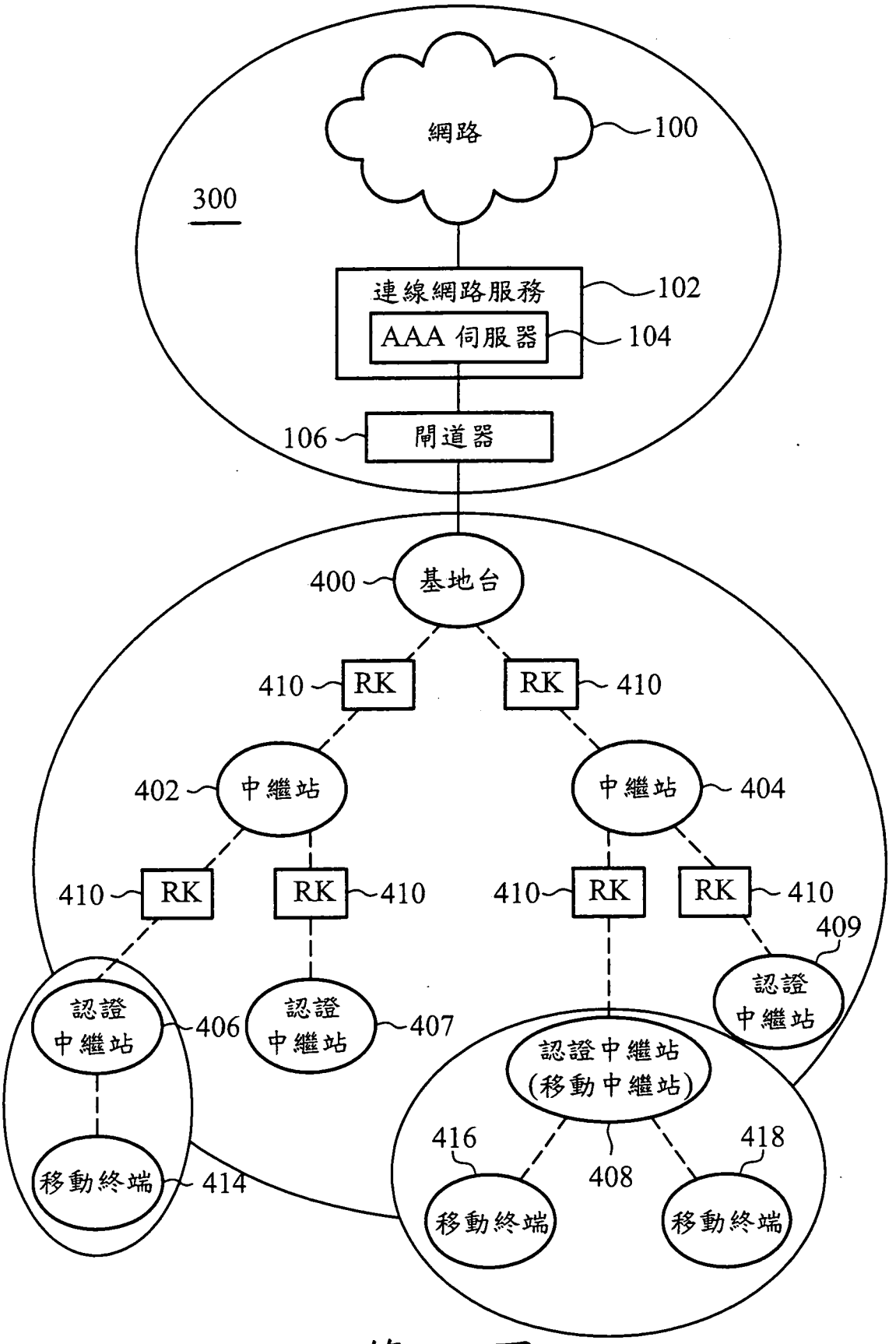
第 1 圖


移動終端
120
111
基地台
106
閘道器
104
連線網路服務
202
204
PKMv2-EAP Start
PKMv2-Req. EAP Transfer
RADIUS-A.-Req.
RADIUS-A.-Req.
PKMv2-Resq. EAP Transfer
RADIUS-A. -Challenge
RADIUS-A. -Challenge
PKMv2-Req. EAP Transfer
RADIUS-A.-Req.
RADIUS-A.-Req.
PKMv2-Resq. EAP Transfer
210
RADIUS-A.-Accept
RADIUS-A.-Accept
MSK
PMK
PKMv2-EAP Complete
210
PMK
206
AK Transfer.
MACK
215
AK
212
AK
MACK
PKMv2-SA-TEK Challenge (RN_B,MAC,AK,AKID)
212
215
PKMv2-SA-TEK Request (RN_B,MAC,AK,AKID)
214
218
PKMv2-SA-TEK Response (MAC,AK,AKID)
KEK
KEK
218
PKMv2-Key-Req. (KEK, M_Nonce)
PKMv2-Key-Reply. (KEK, TEK, B_Nonce)
216
220
PKMv2-Key-Ack
TEK
TEK
220
200

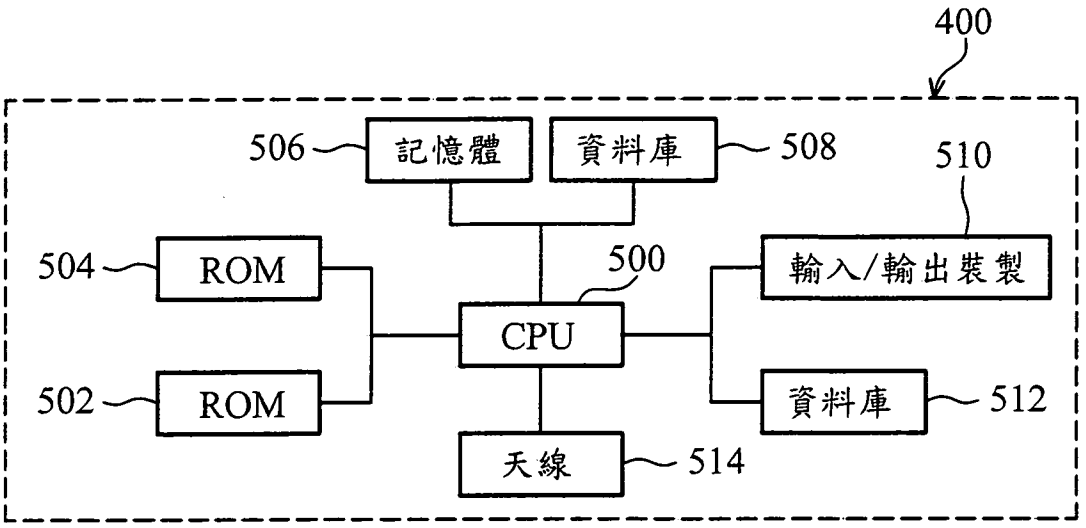
第 2 圖


網路
100
300
連線網路服務
102
AAA 伺服器
104
106
閘道器
310
基地台
311
基地台
312
基地台
313
基地台
320
移動終端
328
中繼站
334
移動
中繼站
330
中繼站
324
移動終端
移動終端
326
332
中繼站
322
移動終端

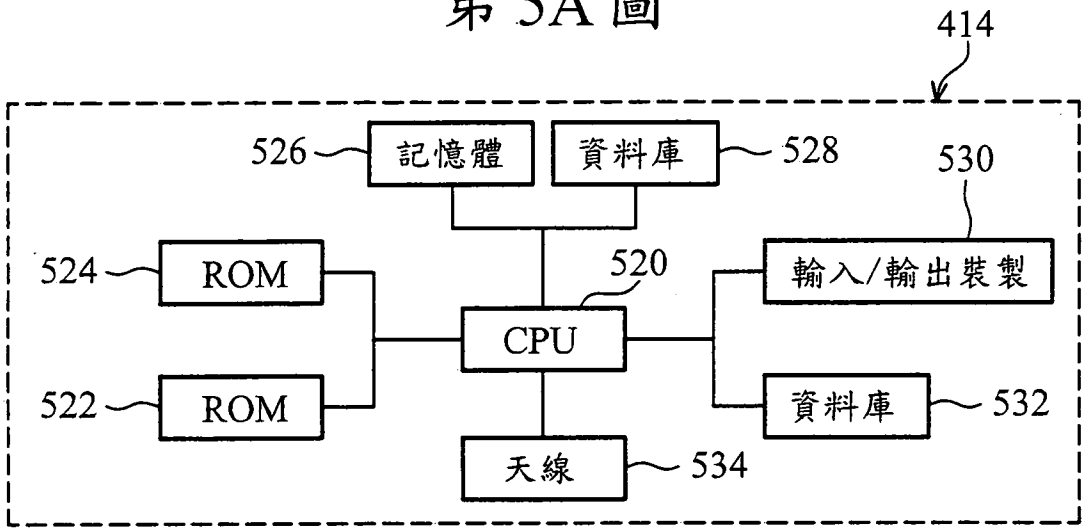
第 3 圖


網路
100
300
連線網路服務
102
AAA 伺服器
104
106
閘道器
400
基地台
410
RK
RK
410
402
中繼站
中繼站
404
410
RK
RK
410
410
RK
RK
410
409
認證
中繼站
406
認證
中繼站
407
認證
中繼站
認證中繼站
(移動中繼站)
416
408
418
移動終端
414
移動終端
移動終端

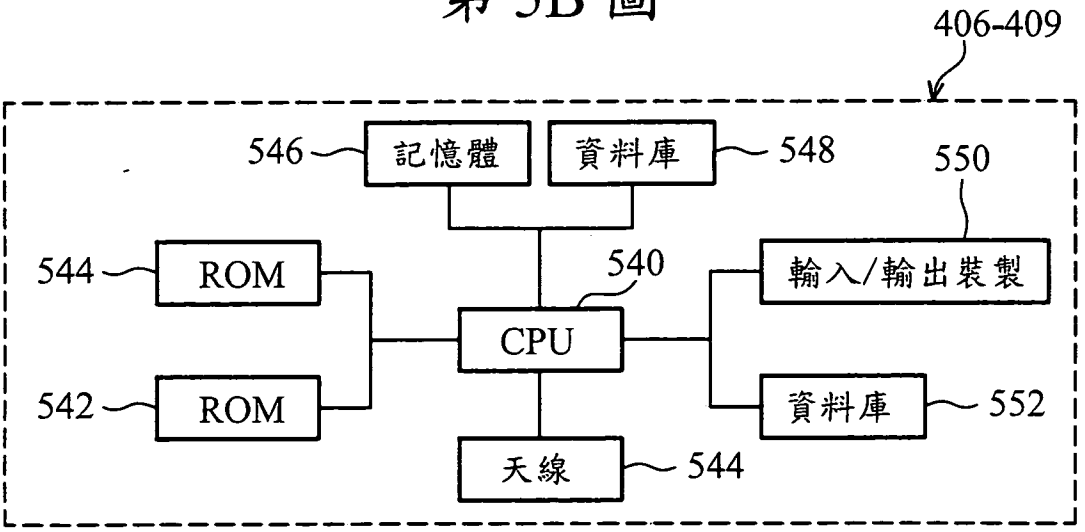
第 4 圖



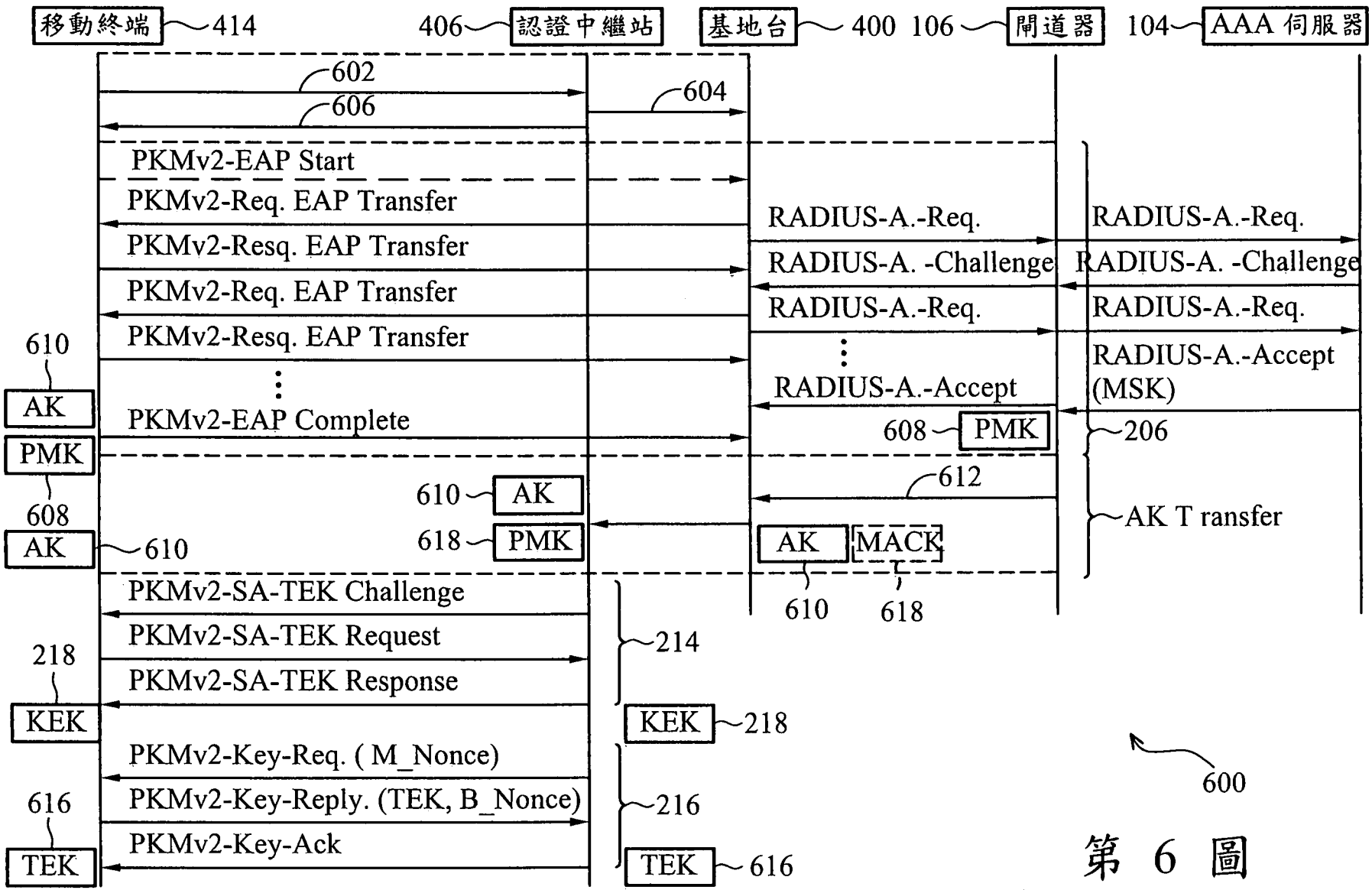

第 5A 圖



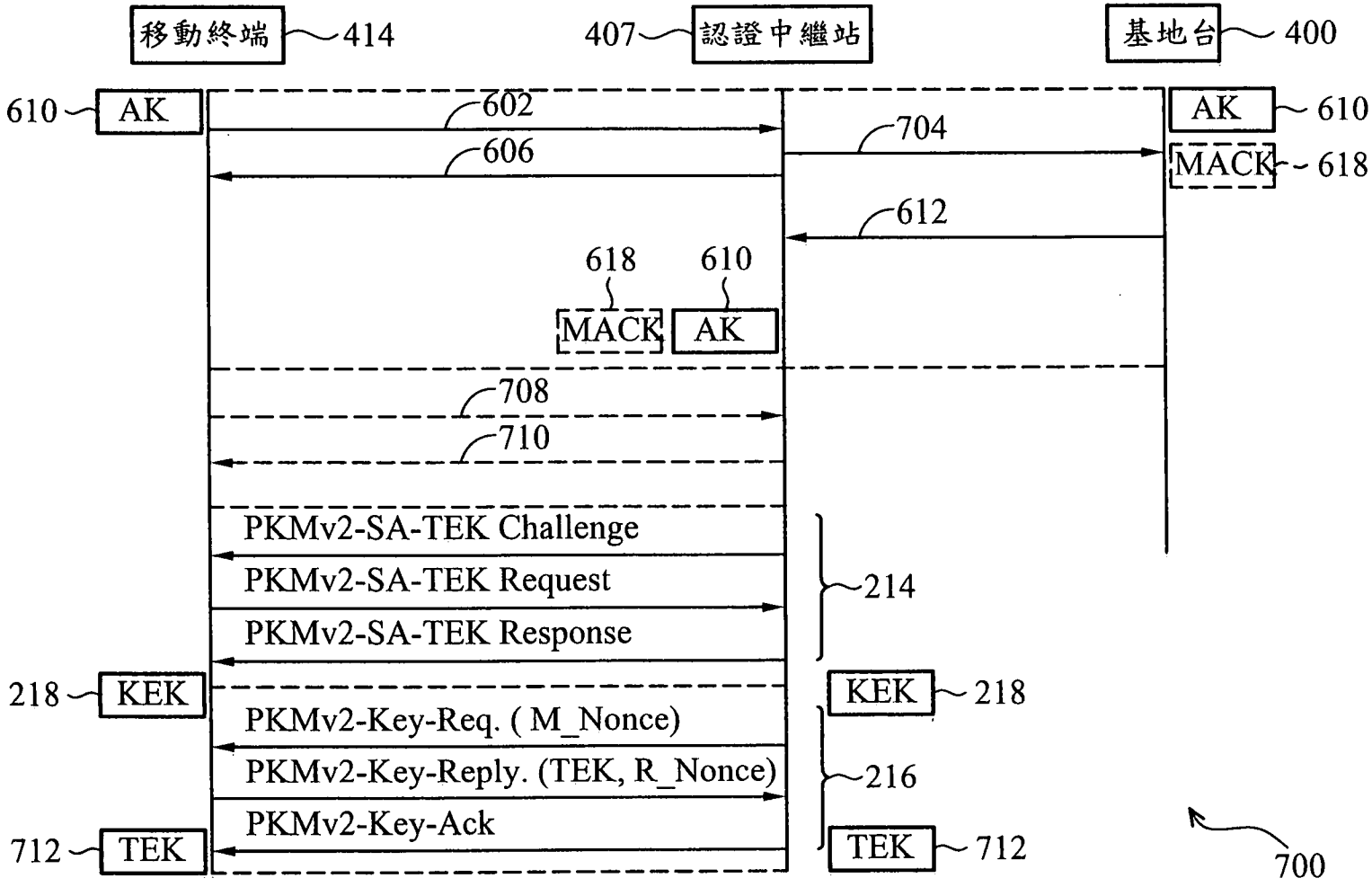

第 5B 圖



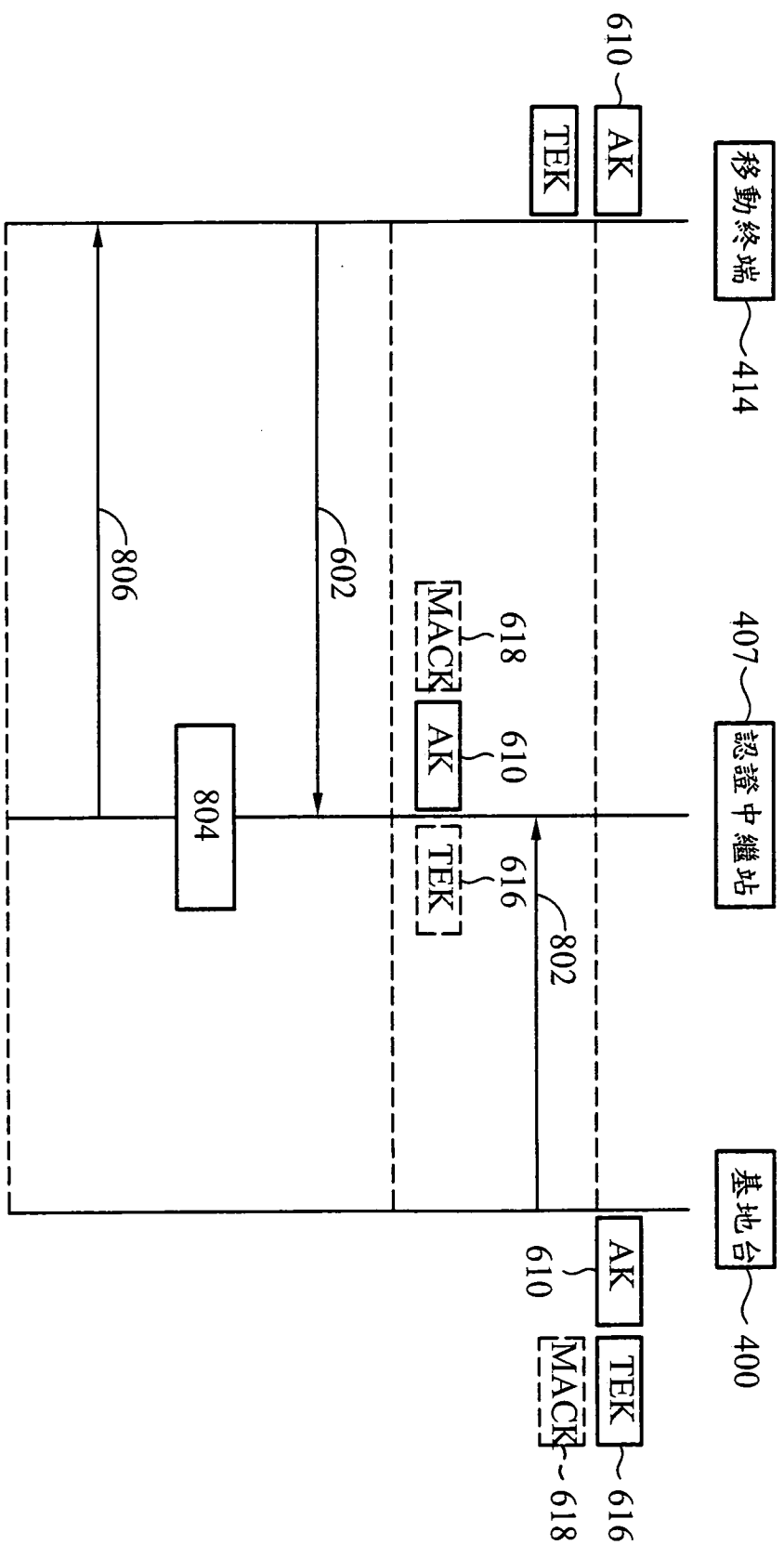

第 5C 圖


移動終端
414
406
認證中繼站
基地台
400
106
閘道器
104
AAA 伺服器
602
604
606
PKMv2-EAP Start
PKMv2-Req. EAP Transfer
PKMv2-Resq. EAP Transfer
PKMv2-Req. EAP Transfer
PKMv2-Resq. EAP Transfer
RADIUS-A.-Req.
RADIUS-A. -Challenge
RADIUS-A.-Req.
RADIUS-A.-Accept
610
AK
PKMv2-EAP Complete
PMK
608
PMK
206
612
610
AK
608
AK
610
618
PMK
AK
MACK
AK T ransfer
610
618
PKMv2-SA-TEK Challenge
PKMv2-SA-TEK Request
214
218
PKMv2-SA-TEK Response
KEK
KEK
218
PKMv2-Key-Req. ( M_Nonce)
616
PKMv2-Key-Reply. (TEK, B_Nonce)
216
PKMv2-Key-Ack
TEK
TEK
616
600

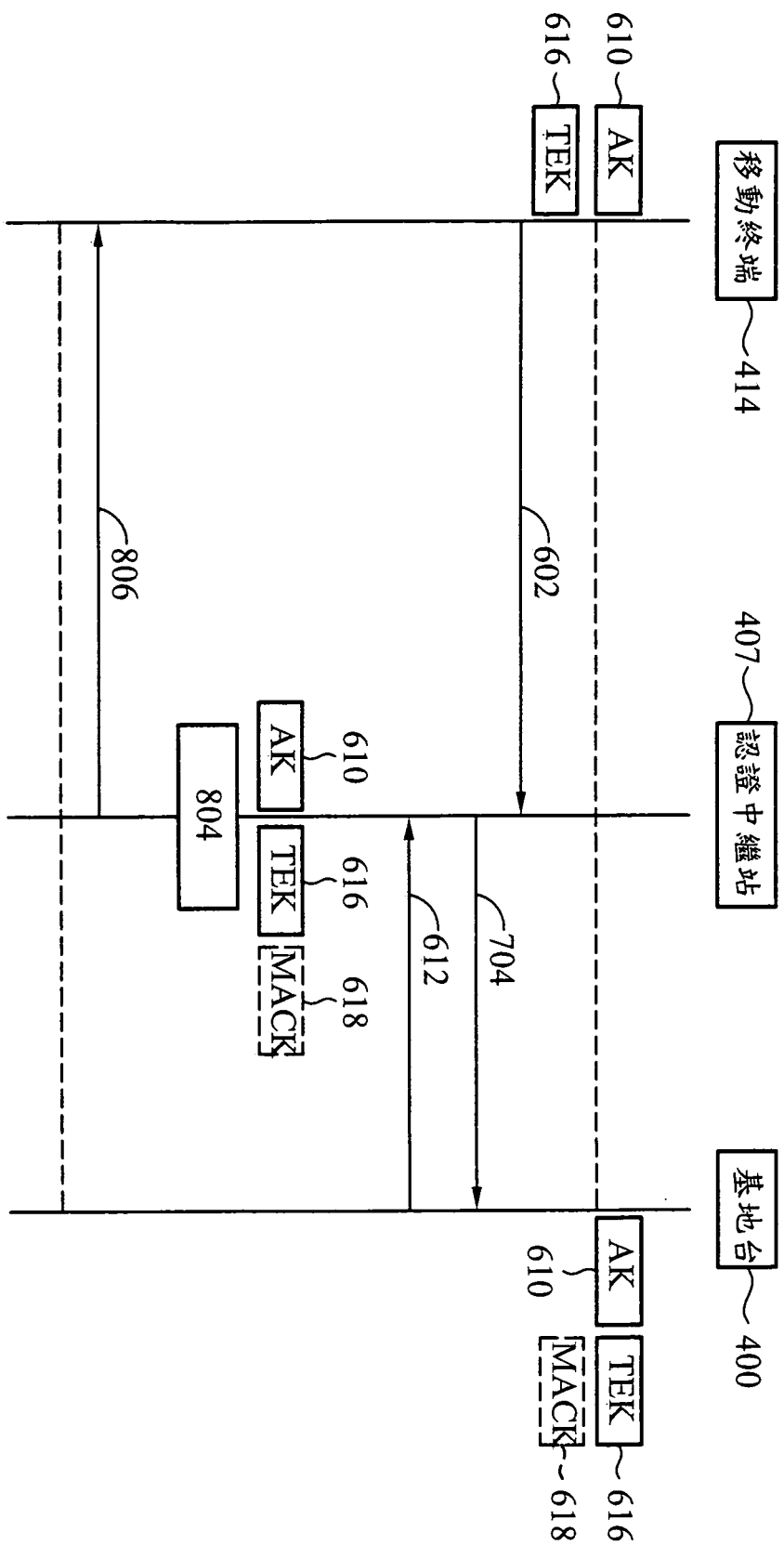
第 6 圖


移動終端
414
407
認證中繼站
基地台
400
610
AK
602
704
AK
610
606
MACK
618
612
618
610
MACK
AK
708
710
PKMv2-SA-TEK Challenge
PKMv2-SA-TEK Request
PKMv2-SA-TEK Response
214
218
KEK
KEK
218
PKMv2-Key-Req. ( M_Nonce)
PKMv2-Key-Reply. (TEK, R_Nonce)
216
PKMv2-Key-Ack
712
TEK
TEK
712
700

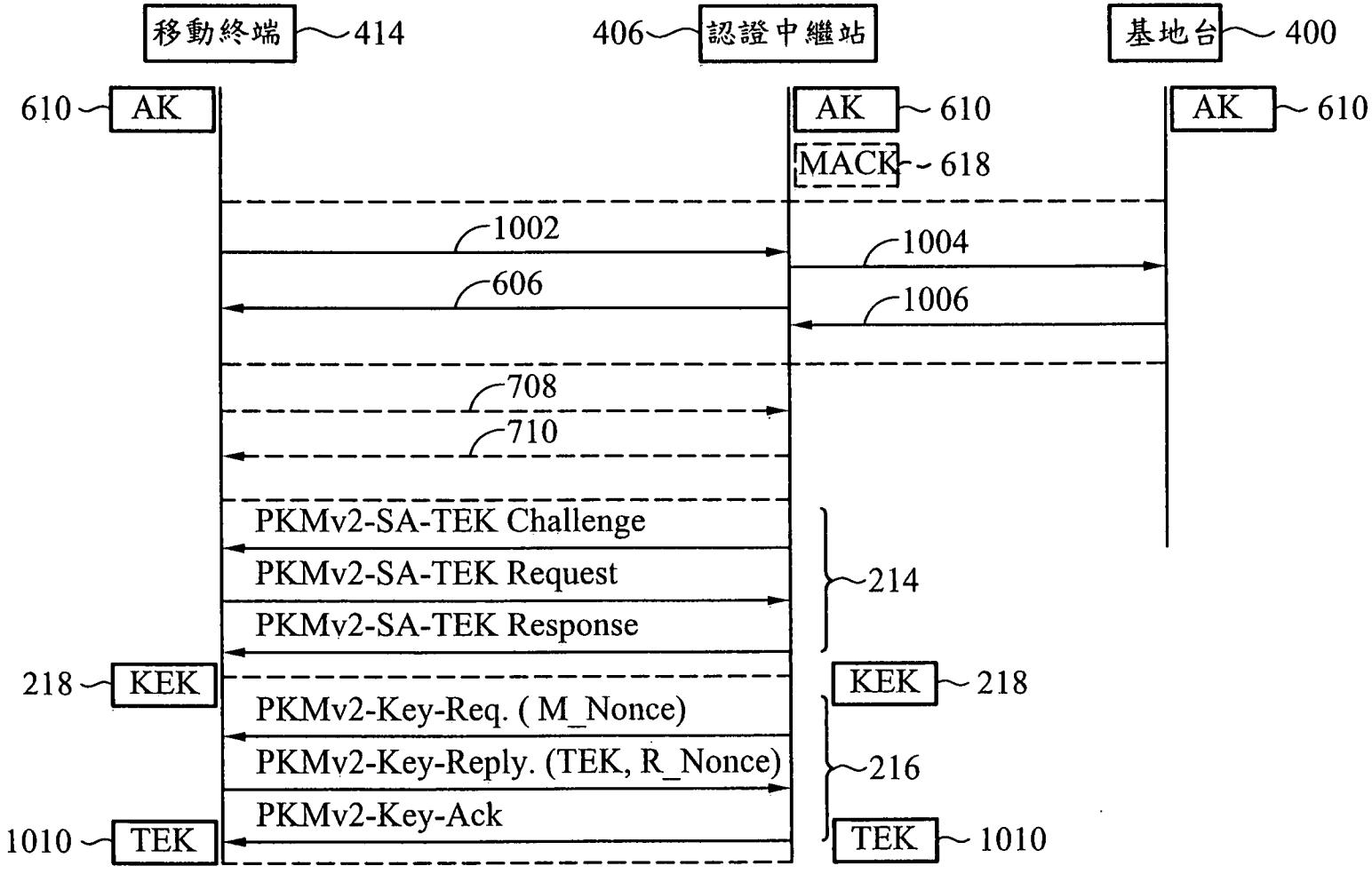
第 7 圖


移動終端
414
610
AK
TEK
認證中繼站
407
618
MACK
610
AK
TEK
616
602
806
804
802
基地台
400
610
AK
MACK
618
TEK
616

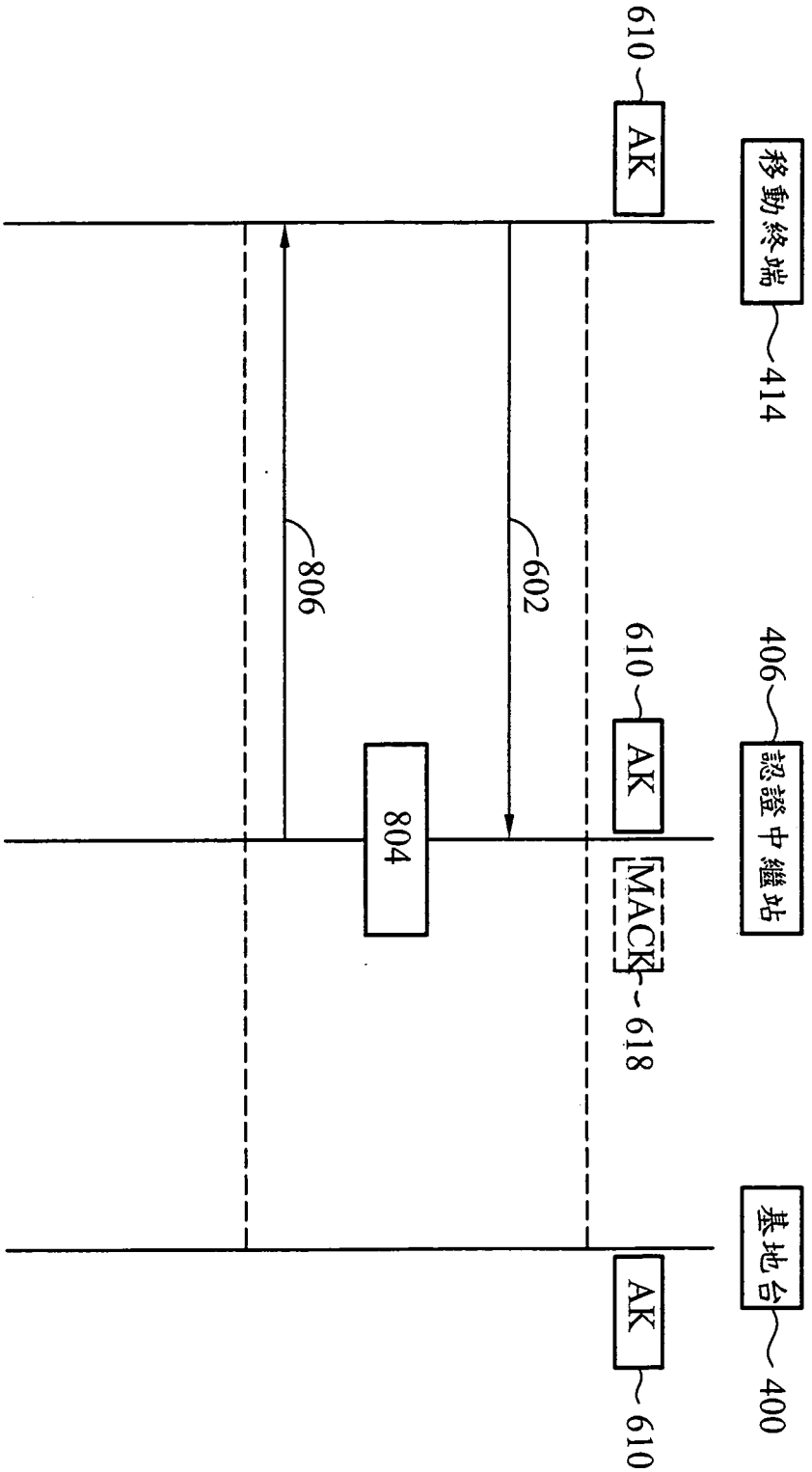
第 8 圖


移動終端
414
認證中繼站
407
基地台
400
610
AK
616
TEK
602
806
804
704
612
618
MACK

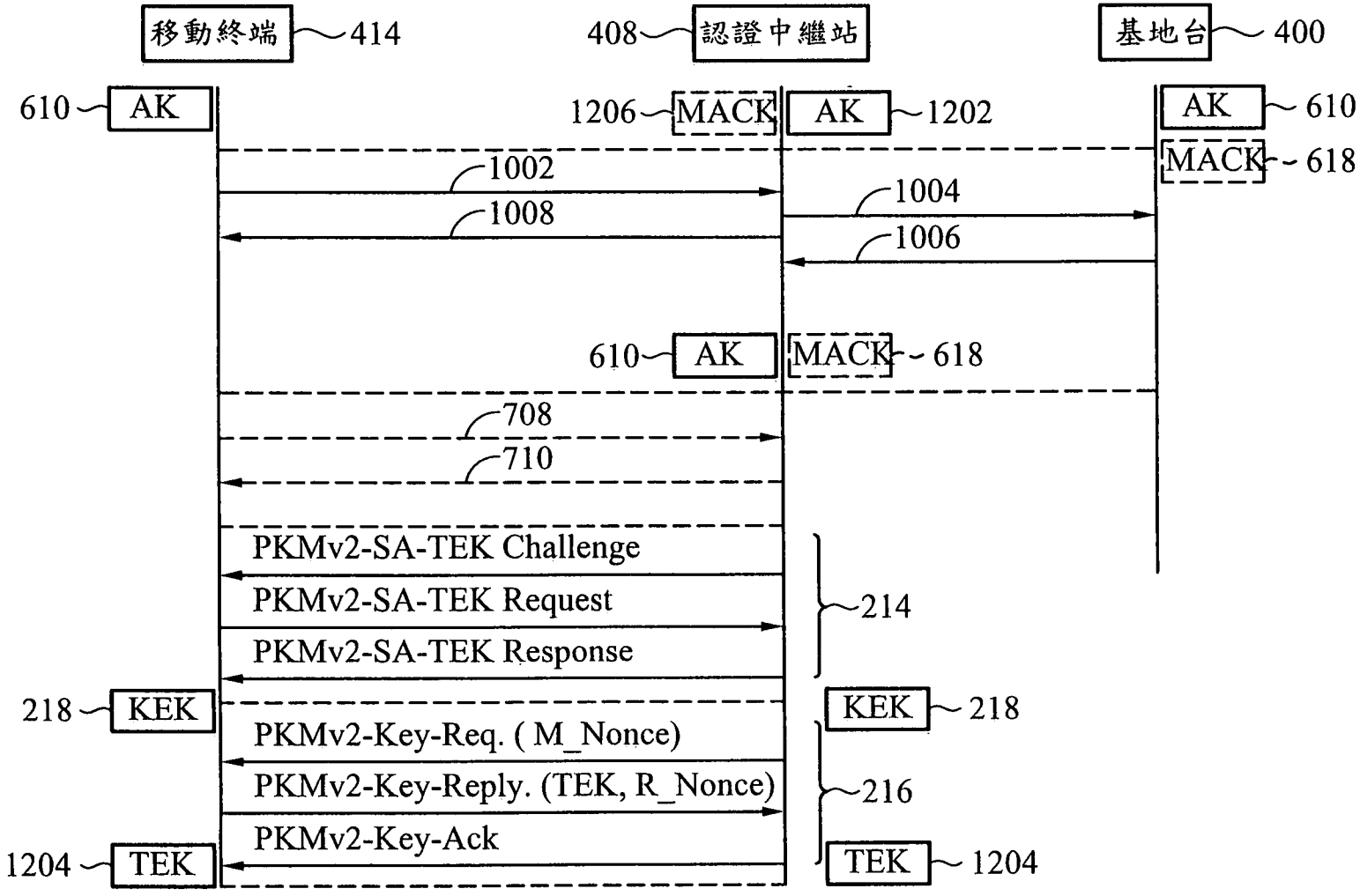
第 9 圖


移動終端
414
406
認證中繼站
基地台
400
610
AK
AK
610
AK
610
MACK
618
1002
1004
606
1006
708
710
PKMv2-SA-TEK Challenge
PKMv2-SA-TEK Request
PKMv2-SA-TEK Response
214
218
KEK
KEK
218
PKMv2-Key-Req. ( M_Nonce)
PKMv2-Key-Reply. (TEK, R_Nonce)
216
PKMv2-Key-Ack
1010
TEK
TEK
1010

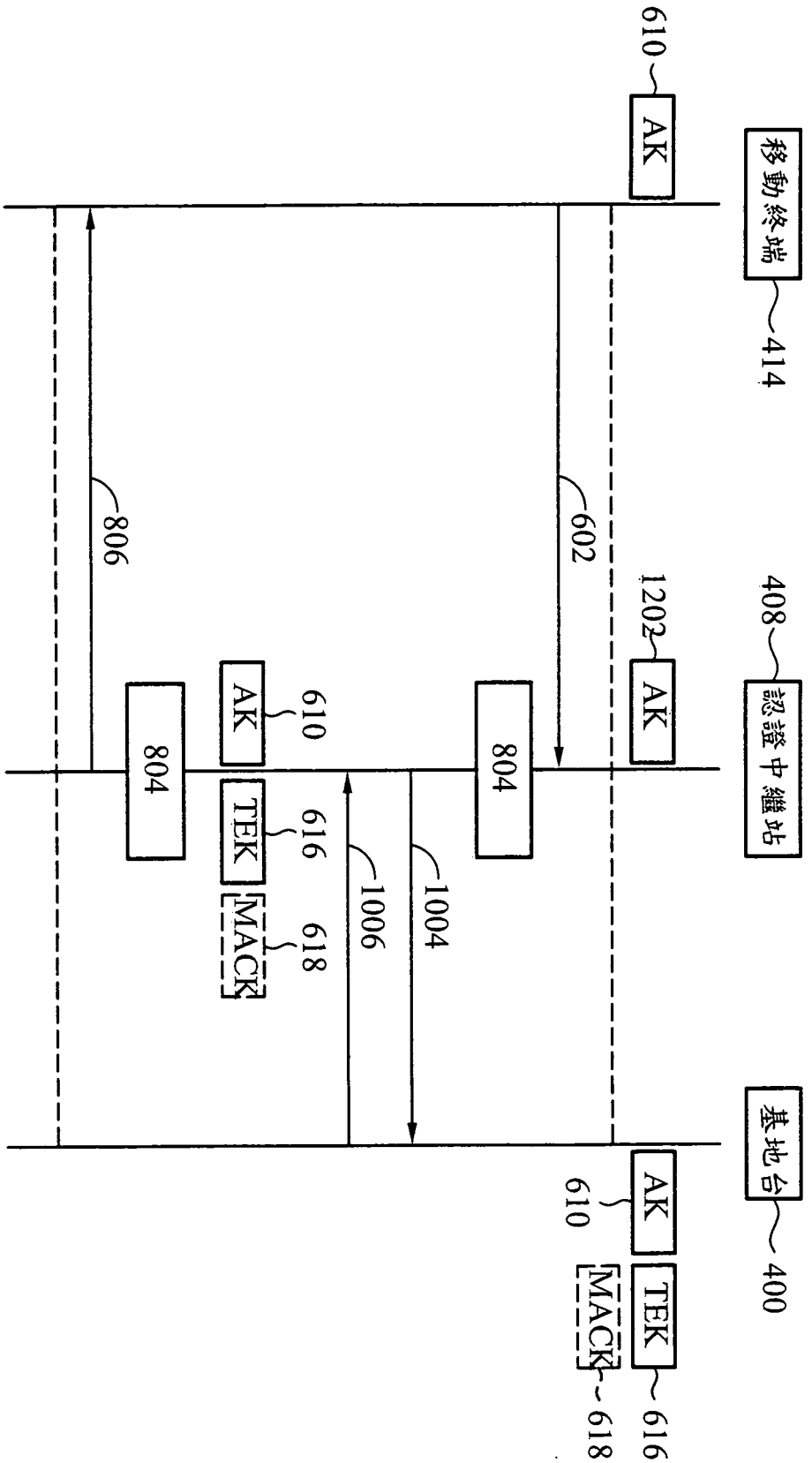
第 10 圖


移動終端
414
610
AK
406
認證中繼站
610
AK
MACK
618
基地台
400
610
AK
602
804
806

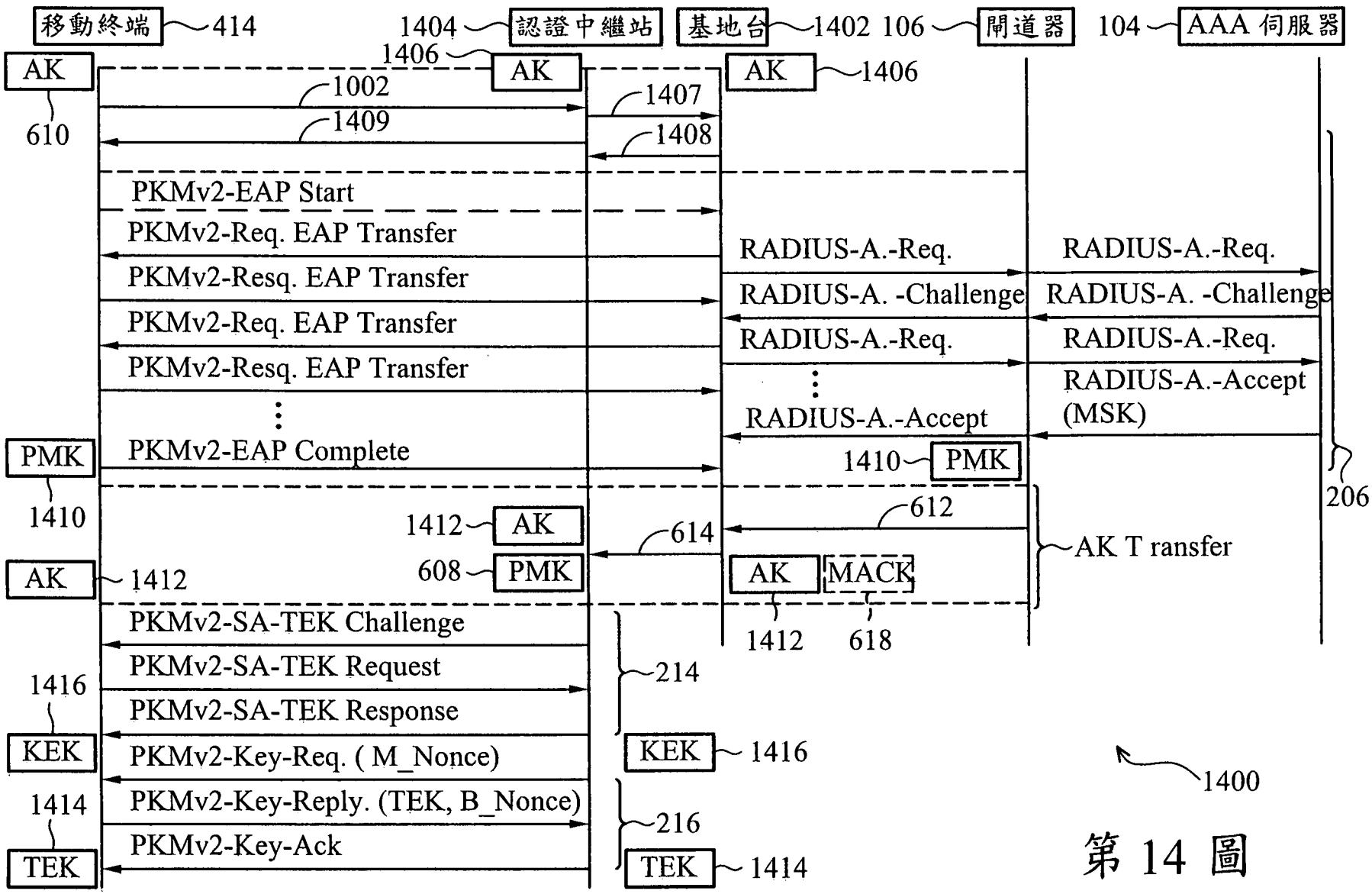
第 11 圖


移動終端
414
408
認證中繼站
基地台
400
610
AK
1206
MACK
AK
1202
AK
610
MACK
618
1002
1004
1008
1006
610
AK
MACK
618
708
710
PKMv2-SA-TEK Challenge
PKMv2-SA-TEK Request
PKMv2-SA-TEK Response
214
218
KEK
KEK
218
PKMv2-Key-Req. ( M_Nonce)
PKMv2-Key-Reply. (TEK, R_Nonce)
PKMv2-Key-Ack
216
1204
TEK
TEK
1204

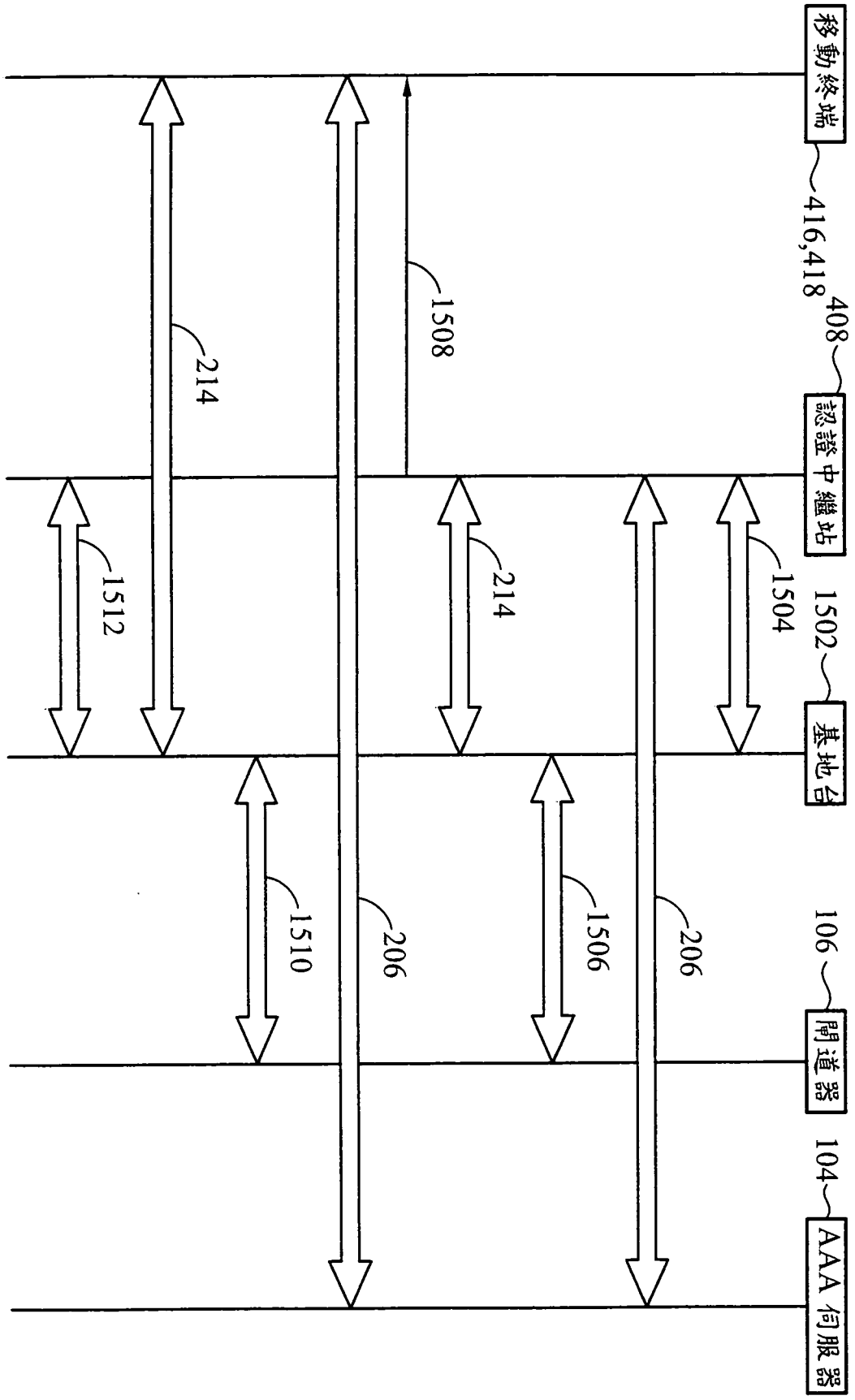
第 12 圖


移動終端
414
610
AK
602
806
804
408
認證中繼站
1202
AK
804
610
AK
TEK
616
MACK
618
1004
1006
基地台
400
AK
610
TEK
616
MACK
618

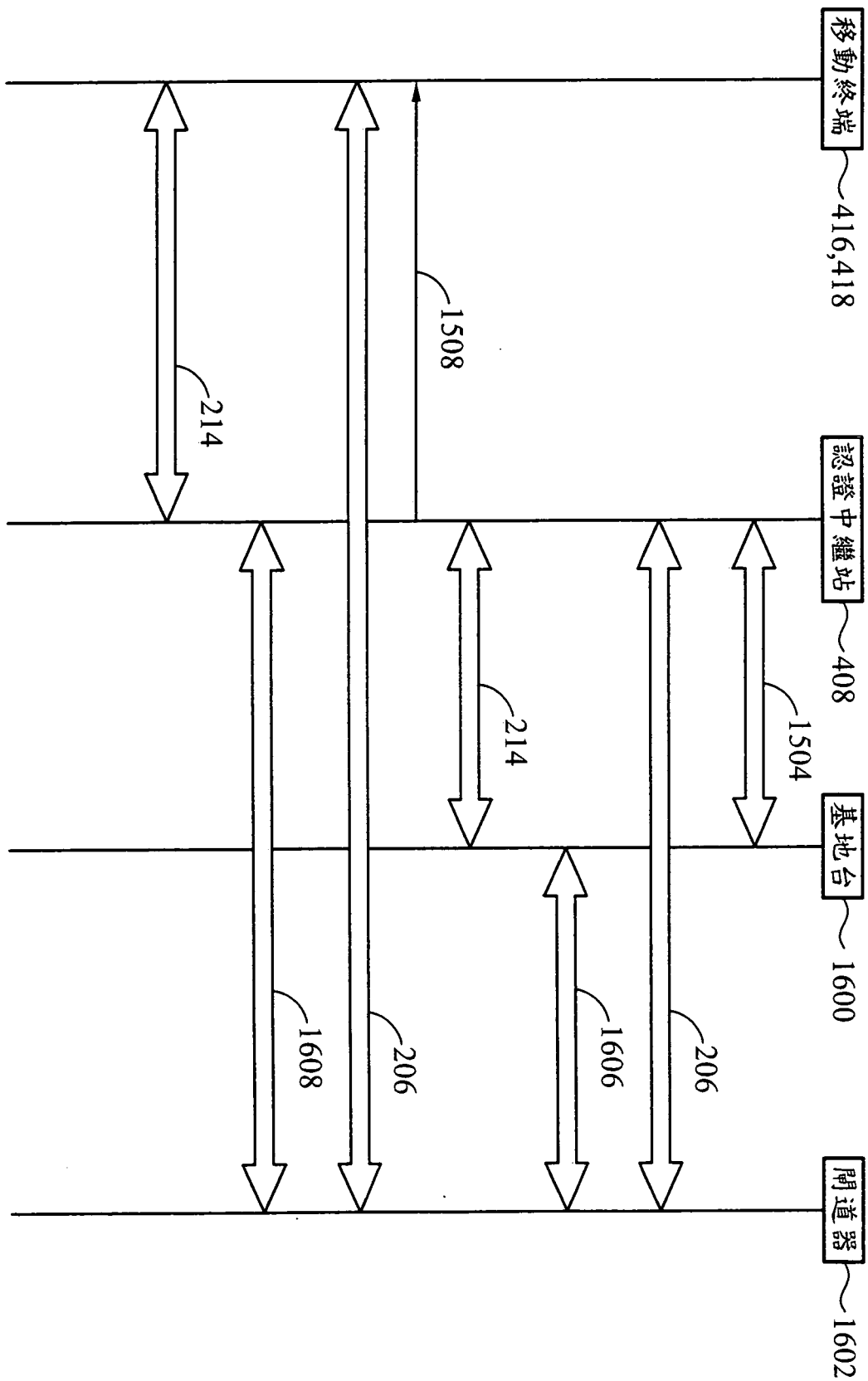
第 13 圖


移動終端
414
1404
認證中繼站
基地台
1402
106
閘道器
104
AAA 伺服器
AK
1406
AK
1406
610
1002
1407
1409
1408
PKMv2-EAP Start
PKMv2-Req. EAP Transfer
RADIUS-A.-Req.
RADIUS-A.-Req.
PKMv2-Resq. EAP Transfer
RADIUS-A. -Challenge
RADIUS-A. -Challenge
PKMv2-Req. EAP Transfer
RADIUS-A.-Req.
RADIUS-A.-Req.
PKMv2-Resq. EAP Transfer
RADIUS-A.-Accept
(MSK)
RADIUS-A.-Accept
PMK
PKMv2-EAP Complete
1410
PMK
206
1410
612
1412
AK
614
AK T ransfer
608
PMK
AK
1412
AK
MACK
1412
618
PKMv2-SA-TEK Challenge
PKMv2-SA-TEK Request
214
1416
PKMv2-SA-TEK Response
KEK
PKMv2-Key-Req. ( M_Nonce)
KEK
1416
1400
1414
PKMv2-Key-Reply. (TEK, B_Nonce)
216
PKMv2-Key-Ack
TEK
TEK
1414

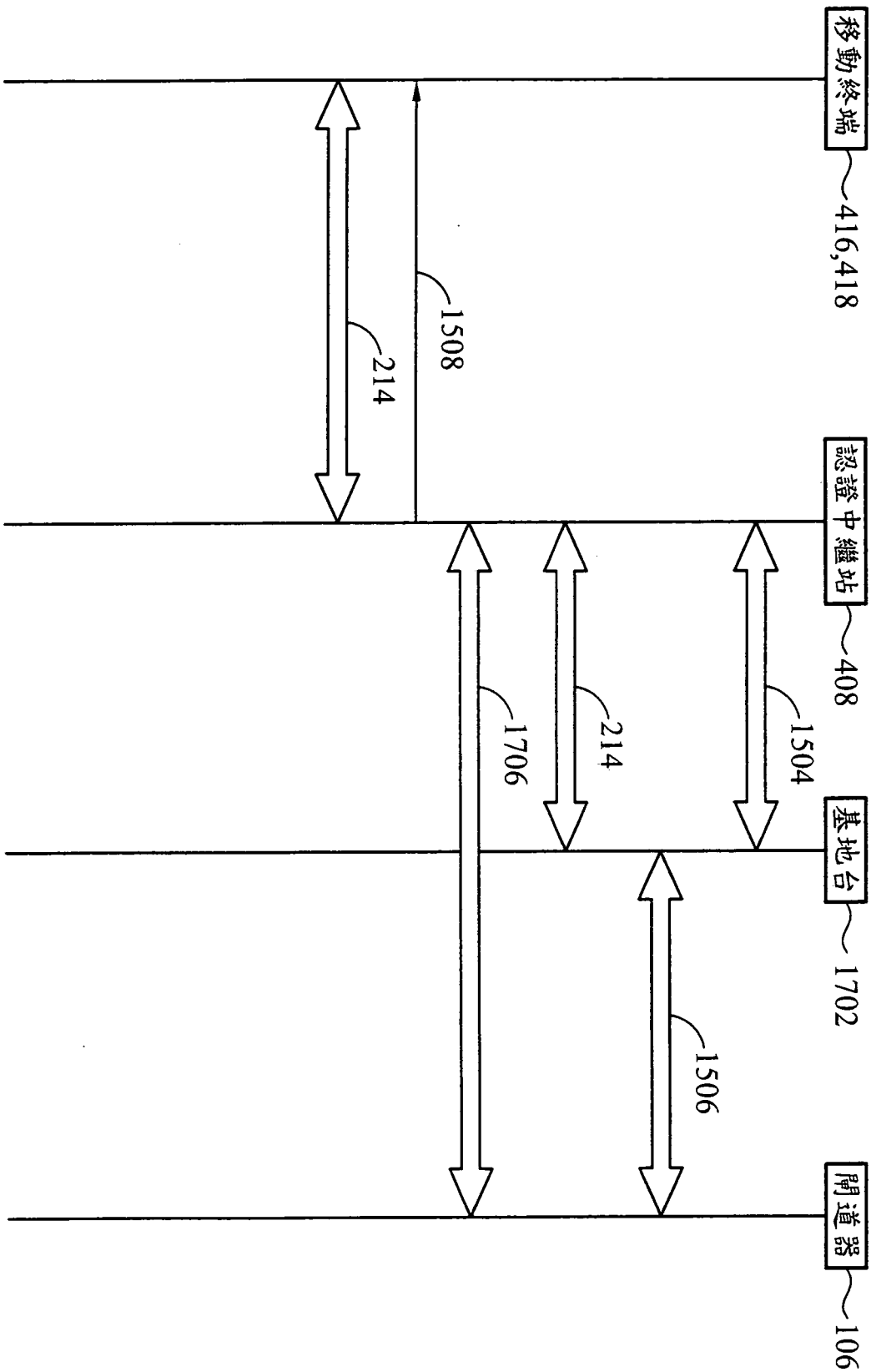
第 14 圖


移動終端
416,418
408
認證中繼站
1502
基地台
106
閘道器
104
AAA 伺服器
1508
214
1504
214
1512
206
1506
206
1510

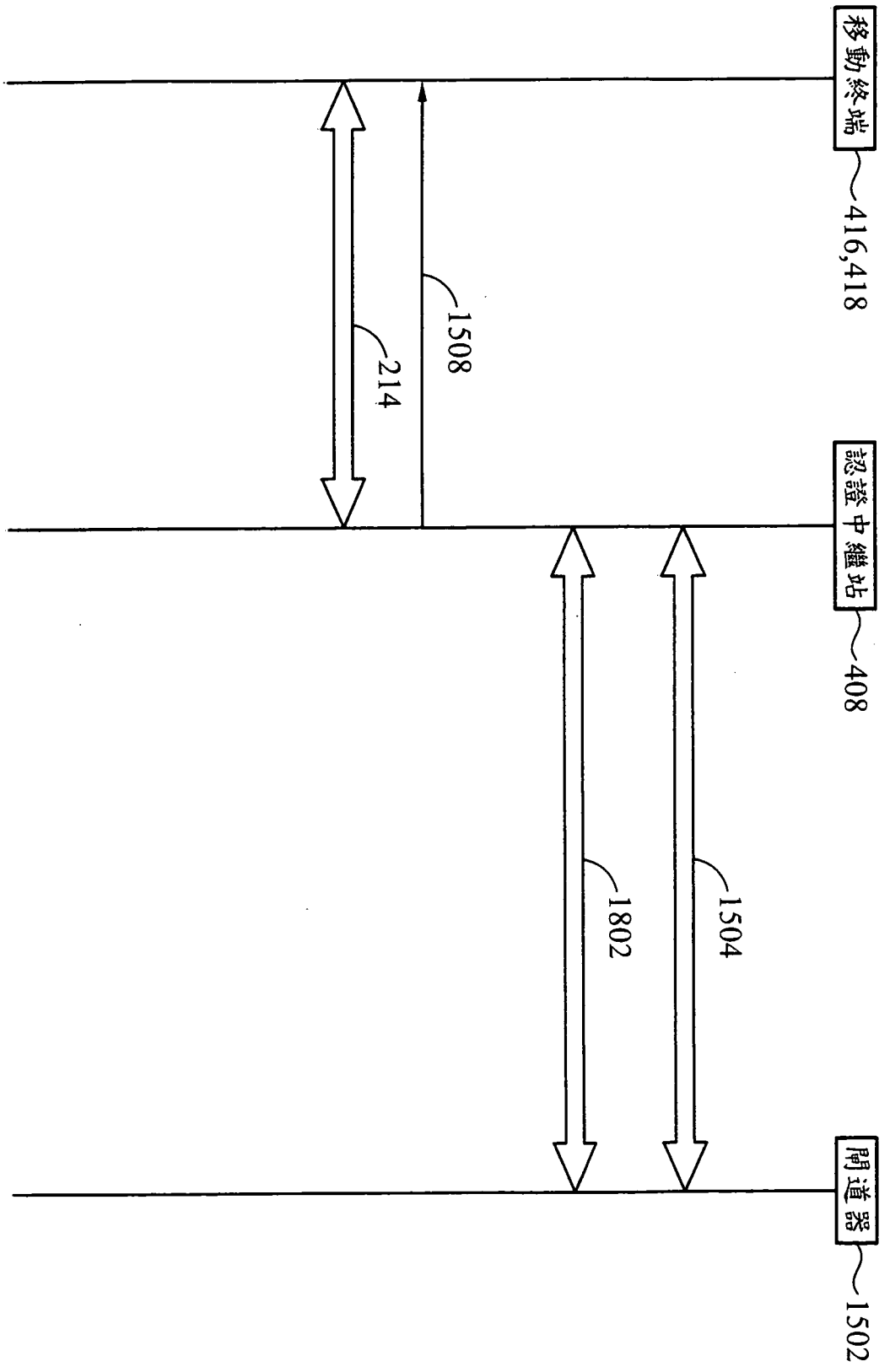
第 15 圖


移動終端
416,418
認證中繼站
408
基地台
1600
閘道器
1602
1508
214
1504
214
206
1606
206
1608

第 16 圖


移動終端
416,418
認證中繼站
408
基地台
1702
閘道器
106
1508
214
1504
214
1706
1506

第 17 圖




第 18 圖