(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 200952425 A1
(43)公開日： 中華民國 98 (2009) 年 12 月 16 日

(21)申請案號：098116890 (22)申請日： 中華民國 98 (2009) 年 05 月 21 日
(51)Int. Cl.： *H04L29/06 (2006.01)* *H04W36/26 (2009.01)*
H04W12/04 (2009.01)
(30)優先權：2008/05/27 美國 12/127,377
(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)
美國
(72)發明人：青山 QING, SHAN (CN) ；金湯姆 CHIN, TOM (US)
(74)代理人：李世章
申請實體審查：有 申請專利範圍項數：28 項 圖式數：8 共 49 頁

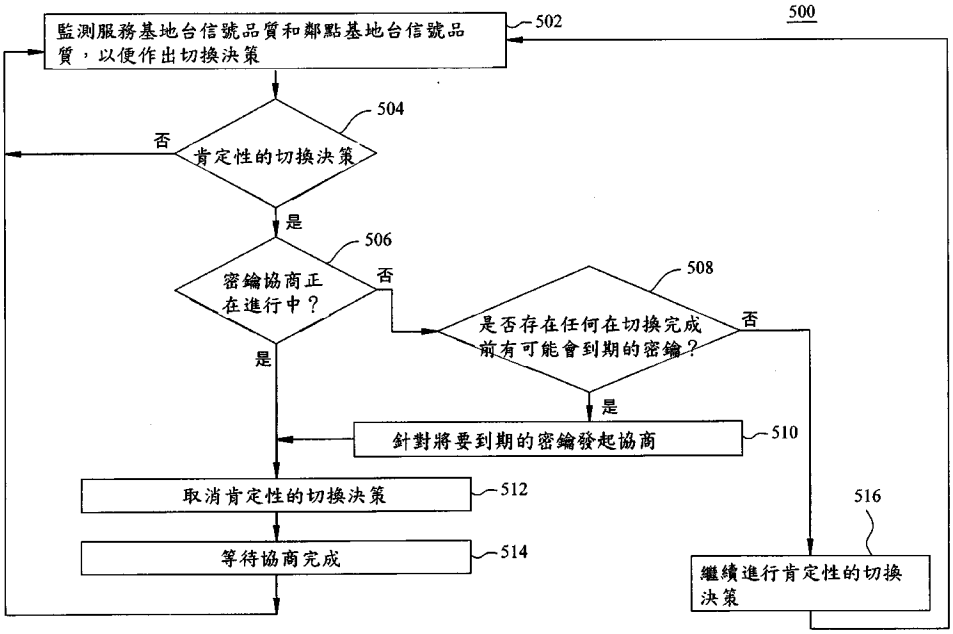
(54)名稱

維持無線通訊安全密鑰的方法和系統

METHODS AND SYSTEMS FOR MAINTAINING SECURITY KEYS FOR WIRELESS COMMUNICATION

(57)摘要

本發明提供了在行動設備狀態或通訊事件(如切換、系統空閒和休眠省電模式等)期間維持安全密鑰的一些實施例。通過監測安全密鑰的生存期，可以刷新密鑰，以確保密鑰生存期在切換過程中或在其他設備不可用的狀態下不會到期。



(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 200952425 A1
(43)公開日： 中華民國 98 (2009) 年 12 月 16 日

(21)申請案號：098116890 (22)申請日： 中華民國 98 (2009) 年 05 月 21 日
(51)Int. Cl.： *H04L29/06 (2006.01)* *H04W36/26 (2009.01)*
H04W12/04 (2009.01)
(30)優先權：2008/05/27 美國 12/127,377
(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)
美國
(72)發明人：青山 QING, SHAN (CN) ；金湯姆 CHIN, TOM (US)
(74)代理人：李世章
申請實體審查：有 申請專利範圍項數：28 項 圖式數：8 共 49 頁

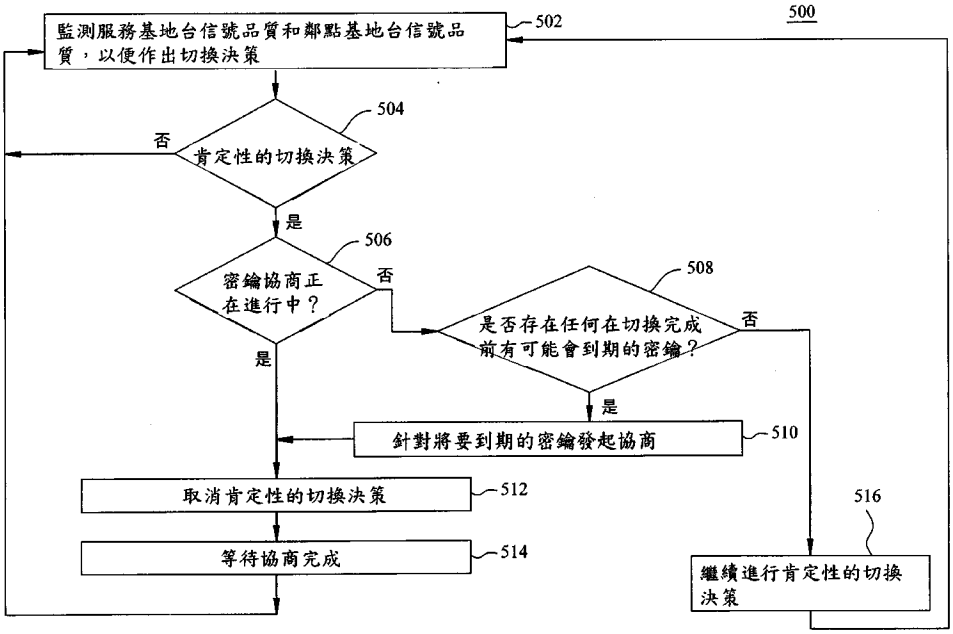
(54)名稱

維持無線通訊安全密鑰的方法和系統

METHODS AND SYSTEMS FOR MAINTAINING SECURITY KEYS FOR WIRELESS COMMUNICATION

(57)摘要

本發明提供了在行動設備狀態或通訊事件(如切換、系統空閒和休眠省電模式等)期間維持安全密鑰的一些實施例。通過監測安全密鑰的生存期，可以刷新密鑰，以確保密鑰生存期在切換過程中或在其他設備不可用的狀態下不會到期。



六、發明說明：

【發明所屬之技術領域】

概括地說，本發明的某些實施例涉及無線通訊，具體地說，本發明的某些實施例涉及維持用於無線通訊的安全密鑰（例如，在無線設備中的移動狀態期間）。

【先前技術】

依據 IEEE 802.16 的 OFDM 無線通訊系統和 OFDMA 無線通訊系統使用多個基地台組成的網路與多個無線設備（即，行動站）進行通訊，其中所述無線設備根據多個次載波頻率的正交性在系統中註冊服務，由此實現所述 OFDM 無線通訊系統和 OFDMA 無線通訊系統，以獲得針對寬頻無線通訊的若干技術優勢（比方說，抗多徑衰落和抗干擾）。每個基地台（BS）向行動站（MS）發送用於傳送資料的射頻（RF）信號，從行動站接收用於傳送資料的射頻信號。在這類系統中，安全協定通常需要網路和行動站共享有效的安全密鑰，諸如 AK 密鑰（授權密鑰）和 TEK 密鑰（訊務加密密鑰）。這些安全密鑰既用於管理連接，還用於傳輸連接。不同的安全密鑰生存期不同，因此標準要求網路和行動站根據密鑰的生存期長度來定期地刷新密鑰。如果在刷新密鑰之前安全密鑰生存期就到期了，那麼行動站和網路之間的通訊將中止，直到成功地協商好新的安全密鑰爲止。

然而，協商新的密鑰會是一個相對冗長的過程，這將破壞用

戶體驗的效果。如果安全密鑰生存期在基地台間切換的過程中到期了，那麼行動站和新基地台之間的通訊將延遲，直到成功地協商好新的安全密鑰爲止，由此，這將會增加切換所引起的任何訊務中斷。

【發明內容】

本發明所闡述的技術使得能夠在各種行動系統狀態或通訊事件（如切換、空閒和休眠模式）期間維持安全密鑰。

某些實施例闡述了維持無線設備用於無線通訊的一或多個安全密鑰的方法，所述方法包括如下操作中之一或如下操作的任意組合：確定通訊事件何時要發生；監測一或多個安全密鑰的生存期，以確定是否存在至少一個安全密鑰在所述通訊事件期間有可能會到期；如果確定出存在所述至少一個安全密鑰有可能會到期，則延遲所述通訊事件；刷新所確定出的有可能會到期的所述至少一個安全密鑰。在某些實施例中，所述方法包括：重複執行確定、監測、延遲、刷新步驟，直到沒有任何安全密鑰被確定爲有可能會到期爲止；啓動所述通訊事件。在某些實施例中，所述通訊事件包括：切換事件、省電模式、休眠模式或空閒模式。在某些實施例中，所述方法包括：依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

某些實施例闡述了維持無線設備用於無線通訊的一或多個安全密鑰的裝置，所述裝置包括如下邏輯中之一或如下邏輯

的任意組合：確定邏輯，用於確定通訊事件何時要發生；監測邏輯，用於監測一或多個安全密鑰的生存期，以確定是否存在至少一個安全密鑰在所述通訊事件期間有可能會到期；延遲邏輯，用於：如果確定出存在所述至少一個安全密鑰有可能會到期，則延遲所述通訊事件；刷新邏輯，用於刷新所確定出的有可能會到期的所述至少一個安全密鑰。在某些實施例中，所述裝置包括：重複執行邏輯，用於重複執行確定邏輯、監測邏輯、延遲邏輯、刷新邏輯，直到沒有任何安全密鑰被確定爲有可能會到期爲止；通訊事件啓動邏輯，用於啓動所述通訊事件。在某些實施例中，所述通訊事件包括：切換事件、省電模式、休眠模式或空閒模式。在某些實施例中，所述裝置包括：通訊邏輯，用於依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

某些實施例闡述了維持無線設備用於無線通訊的一或多個安全密鑰的裝置，所述裝置包括如下構件中之一或如下構件的任意組合：確定構件，用於確定通訊事件何時發生；監測構件，用於監測一或多個安全密鑰的生存期，以確定是否存在至少一個安全密鑰在所述通訊事件期間有可能會到期；延遲構件，用於：如果確定出存在所述至少一個安全密鑰有可能會到期，則延遲所述通訊事件；刷新構件，用於刷新所確定出的有可能會到期的所述至少一個安全密鑰。在某些實施例中，所述裝置包括：重複執行構件，用於重複執行確定構件、監測構件、延遲構件、刷新構件，直到沒有安全密鑰被

確定爲有可能會到期爲止；通訊事件啓動構件，用於啓動所述通訊事件。在某些實施例中，所述通訊事件包括：切換事件、省電模式、休眠模式或空閒模式。在某些實施例中，所述裝置包括：通訊構件，用於依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

某些實施例闡述了維持無線設備用於無線通訊的一或多個安全密鑰的電腦程式產品，包括電腦可讀取媒體，其中所述電腦可讀取媒體包括儲存其上的可由一或多個處理器來執行的指令集，所述指令集包括如下指令中之一或如下指令的任意組合：確定指令，用於確定通訊事件何時發生；監測指令，用於監測一或多個安全密鑰的生存期，以確定是否存在至少一個安全密鑰在所述通訊事件期間有可能會到期；延遲指令，用於：如果確定出存在所述至少一個安全密鑰有可能會到期，則延遲所述通訊事件；刷新指令，用於刷新所確定出的有可能會到期的所述至少一個安全密鑰。在某些實施例中，所述指令集包括：重複執行指令，用於重複執行確定指令、監測指令、延遲指令和刷新指令，直到沒有安全密鑰被確定爲有可能會到期爲止；通訊事件啓動指令，用於啓動通訊事件。在某些實施例中，所述通訊事件包括：切換事件、省電模式、休眠模式或空閒模式。在某些實施例中，所述指令集包括：通訊指令，用於依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

【實施方式】

本發明的某些實施例使得能夠在行動設備的多種狀態或通訊事件（如切換、系統空閒和休眠省電狀態）期間維持安全密鑰。通過監測安全密鑰的生存期，可以刷新密鑰，以確保密鑰生存期在切換過程中或在設備不可用的狀態下不會到期。由此就能避免冗長的安全密鑰協商過程，從而縮短了訊務中斷的總持續時間。

示例性的無線通訊系統

本發明的方法和裝置可在寬頻無線通訊系統中使用。本文所使用的術語「寬頻無線」通常指的是能夠提供多種無線服務（諸如語音、網際網路及/或給定區域內的資料網路存取）的任意組合的技術。

WiMAX（其代表微波存取全球互通）是一種基於多項標準的寬頻無線技術，其能提供長距離高吞吐量寬頻連接。如今，WiMAX主要有兩種應用模式：固定WiMAX和行動WiMAX。舉個例子，固定WiMAX應用模式是一點對多點的，其使得寬頻能夠存取到家庭和企業。行動WiMAX能夠以寬頻速度提供蜂巢網路的完整移動性。

行動WiMAX是基於OFDM（正交分頻多工）和OFDMA（正交分頻多工存取）技術的。OFDM是一種數位多載波調制技術，近來，其廣泛應用於各類高資料率通訊系統中。採用OFDM，可以將一個發射位元流分成多個速率較低的子流。

每個子流調制在多個正交的子流中的一個子流上，並在多個並行的子通道中的一個子通道上進行發送。OFDMA 是一種多工存取技術，在 OFDMA 技術中，用戶分配有不同的時槽中的次載波。OFDMA 是一種靈活的多工存取技術，其能夠在多種多樣的應用、資料率和服務品質要求的情況下容納許多用戶。

在無線通訊服務領域，隨著無線網際網路和無線通訊的迅速發展，對高資料率的需求也日益增長。現今，OFDM/OFDMA 系統被認爲是最具前景的研究領域之一，也是一種針對下一代無線通訊的關鍵技術。這是由於 OFDM/OFDMA 調制方案能夠提供很多優勢，比方說調制效率、頻譜效率、靈活性以及與傳統的單載波調制方案相比而言更强的多徑免疫性。IEEE 802.16x 是新興的標準組織，其用於爲固定寬頻無線存取（BWA）系統和行動寬頻無線存取（BWA）系統定義空中介面。這些標準定義了至少四個不同的實體層（PHY）和一個媒體存取控制（MAC）層。四個實體層中的 OFDM 實體層和 OFDMA 實體層分別是固定 BWA 和行動 BWA 領域中最爲流行的。

圖 1 示出了在其中應用了本發明的實施例的無線通訊系統 100 的例子。無線通訊系統 100 可以是寬頻無線通訊系統。無線通訊系統 100 能夠爲數個細胞服務區 102 提供通訊，其中每一個細胞服務區都由基地台 104 來提供服務。基地台 104 可以是與用戶終端 106 進行通訊的固定站。基地台 104 還可以稱作爲存取點、節點 B 或一些其他術語。

圖 1 描繪了分散在系統 100 當中的多個用戶終端 106。用戶終端 106 可以是固定的（即，靜止的），也可以是移動的。用戶終端 106 還可以稱作爲遠端站、存取終端、終端、用戶單元、行動站、站、用戶裝備等等。用戶終端 106 可以是無線設備，諸如蜂巢式電話、個人數位助理（PDA）、手持設備、無線數據機、膝上型電腦、個人電腦等等。

多種演算法和方法都可用於無線通訊系統 100 中基地台 104 和用戶終端 106 之間的傳輸。例如，可以依據 OFDM/OFDMA 技術在基地台 104 和用戶終端 106 之間收發信號。在這種情況下，無線通訊系統 100 可以稱作爲 OFDM/OFDMA 系統。

有助於從基地台 104 到用戶終端 106 進行傳輸的通訊鏈路稱作爲下行鏈路 108，有助於從用戶終端 106 到基地台 104 進行傳輸的通訊鏈路稱作爲上行鏈路 110。另外，下行鏈路 108 可以稱作爲前向鏈路或前向通道，上行鏈路 110 可以稱作爲反向鏈路或反向通道。

細胞服務區 102 可以劃分成多個扇區 112。扇區 112 是細胞服務區 102 內的實體覆蓋區域。無線通訊系統 100 內的基地台 104 使用的天線將功率流彙集在細胞服務區 102 中的特定扇區 112 內。此類天線可以稱作爲定向天線。

圖 2 示出了在無線通訊系統 100 中使用的無線設備 202 所用的各種部件。無線設備 202 是可用來實現本發明所述的各種方法的設備的例子。無線設備 202 可以是基地台 104，也可以是用戶終端 106。

無線設備 202 包括處理器 204，後者用於控制無線設備 202

的操作。處理器 204 還可以稱作爲中央處理單元（CPU）。記憶體 206 可以既包括唯讀記憶體（ROM），也包括隨機存取記憶體（RAM），其用於向處理器 204 提供指令和資料。記憶體 206 中的一部分還可以包括非揮發性隨機存取記憶體（NVRAM）。一般來說，處理器 204 根據儲存在記憶體 206 中的程式指令來執行邏輯和算術運算。記憶體 206 中的指令可用於實現本發明所述的方法。

無線設備 202 還包括殼體 208，後者包括發射機 210 和接收機 212，用於進行無線設備 202 和遠端站之間的發射和接收。發射機 210 和接收機 212 可以合併成收發機 214。天線 216 連接至殼體 208，並且電耦接到收發機 214。無線設備 202 還可以包括（未示出）多個發射機、多個接收機、多個收發機及/或多個天線。

無線設備 202 還包括信號檢測器 218，後者可用來檢測收發機 214 所接收到的信號位準並對其進行量化。信號檢測器 218 檢測此類信號，諸如總能量、每一僞雜訊（PN）碼片的引導頻能量、功率譜密度和其他信號。無線設備 202 還包括數位信號處理器（DSP）220，後者用於處理信號。

無線設備 202 的各種部件可以通過匯流排系統 222 耦合在一起，其中除資料匯流排之外，匯流排系統 222 還包括電源匯流排、控制信號匯流排和狀態信號匯流排。

圖 3 示出了可用在使用了 OFDM/OFDMA 的無線通訊系統 100 中的發射機 302 的例子。發射機 302 的一部分可以實現在無線設備 202 的發射機 210 中。發射機 302 可以實現在基

地台 104 處，以用於在下行鏈路 108 上向用戶終端 106 發送資料 306。發射機 302 也可以實現在用戶終端 106 處，以用於在上行鏈路 110 上向基地台 104 發送資料 306。

待發送的資料 306 圖示爲串列/並行（S/P）轉換器 308 的輸入。S/P 轉換器 308 將傳輸資料分成 *N* 個並行資料流 310。隨後，將 *N* 個並行資料流 310 作爲輸入提供給映射器 312。映射器 312 將 *N* 個並行資料流 310 映射到 *N* 個星座點上。可以使用一些星座調制方式來完成該映射，如二進位相移鍵控（BPSK）、正交相移鍵控（QPSK）、8 位相移鍵控（8PSK）、正交幅度調制（QAM）等等。由此，映射器 312 輸出 *N* 個並行符號流 316，其中每個符號流 316 都對應於逆快速傅立葉變換（IFFT）320 的 *N* 個正交次載波中的一個次載波。所述 *N* 個並行符號流 316 是在頻域中表示的，可以通過 IFFT 部件 320 將其轉換爲 *N* 個並行時域抽樣流 318。

在此對術語進行簡要解釋。頻域中的 *N* 個並行調制等同於頻域中的 *N* 個調制符號，頻域中的 *N* 個調制符號又等同於頻域中的 *N* 點映射以及 *N* 點 IFFT，頻域中的 *N* 點映射以及 *N* 點 IFFT 又等同於時域中的一個（有效）OFDM 符號，時域中的一個（有效）OFDM 符號又等同於時域中的 *N* 個抽樣。時域中的一個 OFDM 符號 *Ns* 等同於 *Ncp*（每個 OFDM 符號的保護抽樣的數量）+ *N*（每個 OFDM 符號的有效抽樣的數量）。可使用並行/串列（P/S）轉換器 324 將 *N* 個並行時域抽樣流 318 轉換爲 OFDM/OFDMA 符號流 332。保護插入部件 326 在 OFDM/OFDMA 符號流 322 中的連續的 OFDM/OFDMA 符

號之間插入保護間隔。隨後，使用射頻（RF）前端328將保護插入部件326的輸出升頻轉換到期望的發送頻帶。所得到的信號332由天線330隨後發出。

圖3還示出了可用在使用了OFDM/OFDMA的無線設備202中的接收機304的例子。接收機304的一部分可以實現在無線設備202的接收機212中。接收機304可以實現在用戶終端106處，以用於在下行鏈路108上從基地台104接收資料306。接收機304也可以實現在基地台104處，以用於在上行鏈路110上從用戶終端106接收資料306。

所發出的信號332圖示爲在無線通道334上傳送。當天線330'接收到信號332'時，RF前端328'將所接收到的信號332'降頻轉換爲基帶信號。保護移除部件326'隨後移除由保護插入部件326在OFDM/OFDMA符號之間所插入的保護間隔。

將保護移除部件326'的輸出提供至S/P轉換器324'。S/P轉換器324'可以將OFDM/OFDMA符號流分成*N*個並行時域符號流318'，其中每個符號流318'都對應於*N*個正交次載波中的一個次載波。快速傅立葉變換（FFT）部件320'將*N*個並行時域符號流318'變換到頻域，並輸出*N*個並行頻域符號流316'。

解映射器312'執行映射器312所執行的符號映射操作的逆操作，由此輸出*N*個並行資料流310'。P/S轉換器308'將*N*個並行資料流310'合併成單個資料流306'。在理想狀況下，該資料流306'對應於作爲輸入向發射機302提供的資料306。值得注意的是，元件308'、310'、312'、316'、320'、318'

和 324'可以均在基帶處理器 340'中。

在基地台切換過程中維持安全密鑰

IEEE 802.16e-2005 標準支援多種使得行動站能夠在基地台之間進行切換的技術。切換決策可由 BS 或 MS 根據 MS 所報告的測量結果作出。MS 定期地進行 RF 掃描，並定期地測量鄰近基地台的信號品質。例如，可以基於如下情況來作出切換決策：來自一個細胞服務區的信號強度大於當前細胞服務區的信號強度；MS 的位置改變而引起了信號衰落或干擾；MS 需要更高的服務品質（QoS）。無論怎樣，一旦作出了切換決策，MS 就執行如下操作：開始與新的 BS 的下行鏈路傳輸進行同步；如果 MS 在掃描過程中未完成測距（ranging）的話，執行測距；與先前的 BS 斷開連接。

依據 WiMAX 安全協定，在切換之後，與新的 BS 交換資料之前，MS 必須已經建立了有效的安全密鑰。假定在先前商定的一組安全密鑰的生存期結束之前切換過程就已經完成了，那麼，在切換之後就可以立即開始進行資料交換。在另一方面，如果在切換過程中，一或多個安全密鑰的生存期屆滿了，那麼將延遲與新的 BS 的資料交換，直到 MS 能夠與新的 BS 協商好有效的安全密鑰爲止。由此，總的訊務中斷將根據該密鑰協商過程的時間長度而延長，這將足以大大破壞用戶體驗。

圖 4 示出了根據本發明的實施例，在 MS 和 BS 之間協商安全密鑰所需的資訊交互的例子。如圖所示，安全協定要求 BS

和 MS 建立一組不同類型的有效安全密鑰，如 AK 密鑰（授權密鑰）和 TEK 密鑰（訊務加密密鑰）。這些安全密鑰既可用於管理連接，也可用於傳輸連接。

MS 通過向 BS 發送授權請求 402 來協商 AK。作爲回應，BS 產生 AK，並在授權應答 404 中發送相應的密鑰序列號和相應的 AK 的生存期。採用類似的方式，通過向 BS 發送 TEK 密鑰請求 406 來協商 TEK。作爲回應，BS 產生 TEK 密鑰，並在 TEK 密鑰應答 408 中發送 TEK 和相應的 TEK 密鑰的生存期。在建立起有效密鑰之後，MS 和 BS 之間開始進行資料交換 410。

如圖所示，不同安全密鑰的生存期不同（T_{AK} 412 和 T_{TEK} 414），標準要求網路和行動站根據密鑰的生存期長度來定期地刷新密鑰。如果在刷新密鑰之前安全密鑰生存期就屆滿了，那麼 MS 和 BS 之間的通訊將中止，直到成功地協商好了新的安全密鑰爲止。

圖 5 示出了根據本發明的實施例，可在 MS 處執行的用以在基地台之間的切換過程中防止安全密鑰到期的操作 500 的例子。操作 500 從 502 開始，其監測服務基地台和鄰近基地台的信號品質，以便作出切換決策。

在 504，一旦作出了肯定性的切換決策，就在實際發起切換過程之前先檢查安全密鑰生存期的狀態。如果必要的話，就延遲切換過程，以確保建立起有效密鑰並且該有效密鑰在切換過程完成後將依然有效。

舉個例子，根據在 506 所確定的，如果（與當前服務基地台

的）密鑰協商仍在進行當中，那麼就延遲切換過程。例如，在 512，取消肯定性的切換決策，在 514，等待協商完成，由此延遲切換過程。等待直到密鑰協商完成爲止，這樣做能夠確保安全密鑰具有完整的生存期。由此，如果在 504，再次作出肯定性的切換決策，那麼在切換過程完成後密鑰將依然有效。

也可以在 508 檢查密鑰生存期，以判斷是否存在任何密鑰在切換過程完成之前有可能會到期。將密鑰的剩餘生存期與期望的切換時間進行比較（爲穩妥起見，盡可能地考慮到最糟糕的情況），以進行該確定。如果存在一或多個密鑰在切換完成之前有可能會到期，那麼在 510，MS 就發起對要到期的密鑰的協商。在 512，MS 取消肯定性的切換決策，在 514，等待協商完成，從而再次延遲切換過程。

如果（依據 506）沒有待決的密鑰協商，且（依據 508）在切換過程中沒有已到期的或有可能會到期的密鑰，那麼 MS 就在 516 繼續進行肯定性的切換。

圖 6A 和 6B 示出了如何根據圖 5 中的操作來延遲切換過程，從而幫助縮短由於在基地台間進行切換而造成的總訊務中斷時間。首先參照圖 6A，示出了切換過程的圖解的例子，其中安全密鑰在切換過程中到期。

在圖 6A 的例子中，假定在與第一基地台（BS-A）進行正常操作 602 的過程中建立的 TEK 安全密鑰具有生存期 T_{TEK} 610，該生存期在向第二基地台（BS-B）進行切換的過程 604 中屆滿。由於在繼續與 BS-B 進行資料傳輸之前需要有效的

安全密鑰，因此，在切換之後，MS 必須發起密鑰協商 606。這樣一來，總的訊務中斷時間 608_A 將延長至密鑰協商完成後，從而超過了切換時間。

在另一方面，圖 6B 示出了「延遲的」切換過程，其能夠縮短總的訊務中斷 608_B。在圖 6B 的例子中，再次假定在與第一基地台（BS-A）進行正常操作 602 的過程中建立的 TEK 安全密鑰具有生存期 T_{TEK} 610，該生存期在向第二基地台（BS-B）進行切換的過程 604 中屆滿。

然而，通過監測安全密鑰生存期，MS 就能夠確定在切換過程 604 中 TEK 密鑰生存期將有可能會到期。作爲回應，MS 延遲切換過程，並發起密鑰協商 606。在密鑰協商 606 過程中，將要到期的 TEK 密鑰仍然有效，從而，MS 就仍然能夠與 BS-A 交換訊務。由此，在密鑰協商 606 過程中不會出現訊務中斷。

在密鑰協商 606 完成後，MS 將獲得一個新的 TEK 密鑰，該密鑰具有生存期 T_{TEK}, 610'，T_{TEK}, 610'在切換過程 604 之後到期。由此，正常操作 602 就可以（使用新近商定的 TEK 密鑰）在切換過程 604 之後開始進行 MS 和 BS-B 之間的資料交換，而沒有密鑰協商帶來的額外延遲。從而，通過延遲切換過程以刷新將在切換過程中到期的安全密鑰，圖 6B 中的總訊務中斷 608_B 會明顯小於圖 6A 中的總訊務中斷 608_A。

在休眠和空閒狀態下維持安全密鑰

WiMAX 標準定義了省電模式，其允許攜帶型用戶站在 MS

不活躍地發送或接收資料時關閉某些電路來延長電池壽命。比方說，在休眠模式下，MS 在不可用期間，在與服務 BS 協商好的預定時間段（稱作爲休眠窗口），有效地關閉自身。在睡眠視窗之間，（在監聽視窗中）MS 醒來，監測使 MS 退出低功率狀態的訊務或訊息。

休眠視窗可以是固定的，也可以按照指數方式增長，這取決於設備所進入的特定省電類別（PSC）。PSC 類型可根據 MS 在一個特定的連接中所處理的訊務類型來確定。一般來說，PSC I 用於盡力而爲（BE）訊務和非即時可變位元率（NRT-VR）訊務。PSC II 具有固定長度的休眠窗口，一般來說用於主動授權服務（UGS）。PSC III 具有一次性（one-time）休眠窗口，一般來說，其在 MS 知道何時預期到下一個訊務的情況下用於多播訊務或管理訊務。

然而，當 MS 處於不可用的休眠模式下時，安全密鑰有可能會在休眠窗口期間屆滿。就像上文所述的切換過程一樣，如果密鑰在休眠窗口中到期了，那麼在 MS 進入可用間隔（監聽視窗）之後，就需要協商好新的密鑰。如果用戶有待發送的資料，那麼將延遲對該資料的傳輸，直到成功地協商好了新的密鑰爲止，這樣一來會對整個資料吞吐量造成不良影響。這不僅會影響來自 MS 的訊務，還會影響從網路到 MS 的訊務。由此，與在密鑰到期後必須協商密鑰的操作相關聯的延遲會破壞與將要到期的密鑰相關聯的特定服務流的服務品質（QoS）。

然而，本發明的實施例有助於在 MS 處於休眠模式時通過監

測密鑰到期時間來避免所述延遲。如果 MS 在休眠模式下的不可用視窗中檢測到有密鑰將要到期，那麼 MS 就會決定（例如，在發生將導致自然退出的事件之前）提前結束休眠模式，而與網路協商新的密鑰。

圖 7 示出了用於在休眠模式下的不可用時段維持安全密鑰的操作 700 的例子，該操作在 702 啓動。在 704，監測密鑰的剩餘生存期。在 706，判斷在 MS 處於休眠窗口中時在不可用時段期間是否存在任何將要到期的密鑰。將密鑰的剩餘生存期與期望的休眠窗口進行比較，以進行該判斷，比方說，考慮休眠視窗是固定的，還是按照指數方式增長的。如果沒有密鑰可能會到期，那麼就允許設備進入休眠視窗並保持在休眠模式。

在另一方面，如果在休眠窗口中有一或多個密鑰將會到期，那麼在 708，MS 就提前終止休眠模式，在 710，協商一個新的密鑰（或多個密鑰）。提前退出休眠模式以刷新將要到期的密鑰有助於避免會導致資料訊務中斷的冗長的密鑰重新協商過程。在完成了密鑰協商且已刷新了將要到期的密鑰之後，MS 再次啓動休眠模式。

儘管對 WiMAX 標準的當前版本來說是可選的，然而（在 MS 雖未註冊卻仍能接收 DL 廣播訊務的情況下）空閒模式能實現更多的省電，因爲 MS 的部件斷電了。MS 定期地醒來檢查傳呼訊息並更新其傳呼組。

然而，安全密鑰有可能在空閒模式的省電狀態期間屆滿。當用戶想要進行連接時（例如，語音呼叫），如果密鑰確實到

期了，那麼將延遲該連接，直到成功地協商好了新的密鑰爲止。由此，連接建立的時間就延長了，這將會對用戶體驗帶來不良影響。

圖 8 示出了在空閒模式的低功率狀態過程中維持安全密鑰的操作 800 的例子，該操作在 802 啓動。在 804，監測密鑰的剩餘生存期。在 806，判斷在 MS 處於空閒模式的低功率狀態下時是否存在任何將要到期的密鑰。將密鑰的剩餘生存期與低功率狀態的期望持續時間進行比較，以進行該判斷。

如果一或多個密鑰將會到期，那麼在 808，MS 就提前終止空閒模式，在 810，協商一個新的密鑰（或多個密鑰）。提前退出空閒模式以刷新將要到期的密鑰有助於避免冗長的密鑰協商過程，其中該協商過程會導致呼叫建立延遲。在完成了密鑰協商且已刷新了將要到期的密鑰之後，MS 再次進入空閒模式。

上文所述方法的各種操作可由對應於附圖中所示的功能方塊的各種硬體及/或軟體部件及/或模組來執行。一般來說，附圖中所示出的方法都具有相應的配對功能方塊附圖，其中操作方塊對應於具有類似附圖標記的功能方塊。舉個例子，圖 5 中所示的方塊 502-516 對應於圖 5A 中所示的功能方塊 502A-516A。

資訊和信號可以使用多種不同的技術和方法來表示。例如，在貫穿上文的描述中提及的資料、指令、命令、資訊、信號等可以用電壓、電流、電磁波、磁場或粒子、光場或粒子或其任意組合來表示。

用於執行本發明所述功能的通用處理器、數位信號處理器（DSP）、專用積體電路（ASIC）、現場可程式閘陣列（FPGA）或其他可程式邏輯器件（PLD）、個別閘門或者電晶體邏輯器件、個別硬體部件或其任意組合，可以實現或執行結合本發明而描述的各種示例性邏輯方塊、模組和電路。通用處理器可以是微處理器，或者，該處理器也可以是任何商用處理器、控制器、微控制器或者狀態機。處理器也可能實現爲計算設備的組合，例如，DSP和微處理器的組合、多個微處理器、一或多個微處理器與DSP內核的結合，或者任何其他此種結構。

結合本發明所描述的方法或者演算法的步驟可直接體現爲硬體、由處理器執行的軟體模組或其組合。軟體模組可以位於本領域所熟知的任何形式的儲存媒體中。可使用的一些儲存媒體的例子包括隨機存取記憶體（RAM）、唯讀記憶體（ROM）、快閃記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、可移除磁碟、CD-ROM等等。軟體模組可以包括單個指令，也可以包括許多指令，其還可以分散於若干不同的代碼段、不同的程式以及多個儲存媒體中。儲存媒體可以耦接至處理器，從而使處理器能夠從該儲存媒體讀取資訊，且可向該儲存媒體寫入資訊。當然，儲存媒體也可以是處理器的組成部分。

本發明所公開的方法包括用於實現本發明所述的方法的一或多個步驟或動作。在不脫離請求項範圍的情況下，方法步驟及/或動作可以彼此間相互交換。換言之，除非指定了步驟

或動作的特定次序，否則就可以在不脫離請求項範圍的情況下，修改特定步驟及/或動作的次序及/或應用。

本發明所述功能可以用硬體、軟體、韌體或它們組合的方式來實現。當使用軟體實現時，可以將這些功能作爲指令、一組或多組指令儲存在電腦可讀取媒體或儲存媒體中。儲存媒體可以是電腦或一或多個處理設備能夠存取的任何可用媒體。通過示例的方式而非限制的方式，這種電腦可讀取媒體可以包括 RAM、ROM、EEPROM、CD-ROM 或其他光碟儲存、磁片儲存媒體或其他磁碟儲存裝置、或者能夠用於攜帶或儲存期望的指令或資料結構形式的程式碼並能夠由電腦進行存取的任何其他媒體。如本發明所使用的，盤和碟包括壓縮光碟（CD）、鐳射影碟、光碟、數位多功能光碟 (DVD)、軟碟和藍光碟，其中盤（disk）通常磁性地複製資料，而碟（disc）則用鐳射來光學地複製資料。

軟體或指令還可以經由傳輸媒體來發送。例如，如果軟體是使用同軸電纜、光纖電纜、雙絞線、數位用戶線（DSL）或者諸如紅外線、無線和微波之類的無線技術從網站、伺服器或其他遠端源發送的，那麼同軸電纜、光纖電纜、雙絞線、DSL 或者諸如紅外線、無線和微波之類的無線技術包括在所述傳輸媒體的定義中。

此外，應當認識到，如果適當的話，用戶終端及/或基地台可以下載及/或得到用於執行本發明所述的方法和技術的模組及/或適當的手段。例如，可以將此類設備耦接至伺服器，以便轉移用於執行本發明所述方法的手段。另外，本發明所述

的各種方法可以通過儲存單元（例如，RAM、ROM、諸如壓縮光碟（CD）或軟碟的實體儲存媒體等等）來提供，從而用戶終端及/或基地台就能夠通過耦接到該設備或通過向該設備提供儲存單元來獲得各種方法。此外，也可以使用可用來向設備提供本發明所述的方法和技術的任何其他合適的技術。

應當理解，所述請求項並不限於上文所闡述的精確的構造和部件。在不脫離本發明請求項的範圍的情況下，可以對上文所描述的方法和裝置的排列、操作和細節作出各種修改、改變和變形。

【圖式簡單說明】

通過參考實施例，能夠獲得對上述本發明的各種特徵的更詳細的理解和對上文所簡要歸納的說明的更具體的說明，其中一些實施例示出在附圖中。然而，應當注意的是，附圖僅僅示出了本發明的某些典型的實施例，因此不應當將其視爲限制了本發明的範圍，因爲附圖說明也適用於其他等效的實施例。

圖 1 示出了根據本發明某些實施例的示例性無線通訊系統。

圖 2 示出了根據本發明某些實施例的可在無線設備中使用的各種部件。

圖 3 示出了根據本發明某些實施例的可在無線通訊系統中使用的示例性發射機和示例性接收機，其中該無線通訊系統使用的是正交分頻多工和正交分頻多工存取（OFDM/OFDMA）技術。

圖 4 示出了根據本發明某些實施例的行動站和基地台之間的用以協商安全密鑰的資訊交互的例子。

圖 5 示出了根據本發明實施例的用於在基地台間的切換過程中維持安全密鑰的示例性操作。

圖 5A 是能夠執行圖 5 中的示例性操作的部件的方塊圖。

圖 6A&6B 根據本發明的實施例分別示出了在正常切換和延遲切換過程中的中斷的例子。

圖 7 示出了根據本發明實施例的用於在休眠模式下的不可用時段中維持安全密鑰的示例性操作。

圖 7A 是能夠執行圖 7 中的示例性操作的部件的方塊圖。

圖 8 示出了根據本發明實施例的用於在空閒模式下的不可用時段中維持安全密鑰的示例性操作。

圖 8A 是能夠執行圖 8 中的示例性操作的部件的方塊圖。

【主要元件符號說明】

100	無線通訊系統
102	細胞服務區
104	基地台
106	用戶終端
108	下行鏈路
110	上行鏈路
112	扇區
202	無線設備
204	處理器
206	記憶體
208	殼體
210	發射機
212	接收機
214	收發機
216	天線
218	信號檢測器
220	DSP

222	匯流排系統
302	發射機
306	資料
306'	資料流
308	S/P 轉換器
308'	P/S 轉換器
310	並行資料流
310'	並行資料流
312	映射器
312'	解映射器
316	並行符號流
316'	並行頻域符號流
318	並行時域抽樣流
318'	並行時域符號流
320	IFFT 部件
320'	FFT 部件
322	OFDM/OFDMA 符號流
324	P/S 轉換器
324'	S/P 轉換器
326	保護插入部件
326'	保護移除部件
328	RF 前端
328'	RF 前端
330	天線

330'	天線
332	OFDM/OFDMA 符號流
332'	信號
334	無線通道
402	授權請求
404	授權應答
406	TEK 密鑰請求
408	TEK 密鑰應答
410	資料交換
412	生存期 T_{AK}
414	生存期 T_{TEK}
502A	構件
504A	構件
506A	構件
508A	構件
510A	構件
512A	構件
514A	構件
516A	構件
602	正常操作
604	進行切換
606	密鑰協商
608	總的訊務中斷時間
610	生存期

702A	構件
704A	構件
708A	構件
710A	構件
800A	構件
802A	構件
804A	構件
808A	構件
810A	構件

200952425

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：98116890

※ 申請日期：2009 年 5 月 21 日　　※IPC 分類：H04L 29/06 (2006.01)
H04W 36/36 (2009.01)
H04W 12/04 (2009.01)

一、發明名稱：（中文/英文）

維持無線通訊安全密鑰的方法和系統

METHODS AND SYSTEMS FOR MAINTAINING SECURITY KEYS FOR WIRELESS COMMUNICATION

二、中文發明摘要：

本發明提供了在行動設備狀態或通訊事件（如切換、系統空閒和休眠省電模式等）期間維持安全密鑰的一些實施例。通過監測安全密鑰的生存期，可以刷新密鑰，以確保密鑰生存期在切換過程中或在其他設備不可用的狀態下不會到期。

三、英文發明摘要：

Certain embodiments allow security keys to be maintained across mobile device states, or communication events, such as hand-over, and system idle and sleep power savings modes. By monitoring the lifetime of security keys, keys may be

refreshed in an effort to ensure key lifetimes will not expire during a hand-over process or other device unavailable state.

七、申請專利範圍：

1、一種維持一無線設備用於無線通訊的一或多個安全密鑰的方法，包括以下步驟：

確定一通訊事件何時要發生；

監測該一或多個安全密鑰的生存期，以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期；

如果確定出該至少一個安全密鑰可能會到期，則延遲該通訊事件；以及

刷新所確定出的可能會到期的該至少一個安全密鑰。

2、根據請求項1之方法，還包括以下步驟：

重複執行該等確定、監測、延遲、刷新步驟，直到確定出沒有任何安全密鑰可能會到期爲止；以及

啓動該通訊事件。

3、根據請求項1之方法，其中：

該通訊事件是一切換事件；以及

監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期，包括：

將該至少一個安全密鑰的一剩餘生存期與該切換事件的一預期持續時間進行比較。

4、根據請求項1之方法，其中：

該通訊事件是一省電模式；以及

監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期，包括：

將該至少一個安全密鑰的一剩餘生存期與該省電模式的一低功率狀態的一時段進行比較。

5、根據請求項4之方法，其中該省電模式包括一休眠模式。

6、根據請求項4之方法，其中該省電模式包括一空閒模式。

7、根據請求項1之方法，其中依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，該無線設備使用訊框來進行通訊。

8、一種維持一無線設備用於無線通訊的一或多個安全密鑰的裝置，包括：

確定邏輯，用於確定一通訊事件何時要發生；

監測邏輯，用於監測該一或多個安全密鑰的生存期，以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期；

延遲邏輯，用於：如果確定出該至少一個安全密鑰可能會到期，則延遲該通訊事件；以及

刷新邏輯，用於刷新所確定出的可能會到期的該至少一個安全密鑰。

9、根據請求項8之裝置，還包括：

重複執行邏輯，用於重複執行該確定邏輯、該監測邏輯、該延遲邏輯、該刷新邏輯，直到確定出沒有任何安全密鑰可能會到期爲止；以及

通訊事件啓動邏輯，用於啓動該通訊事件。

10、根據請求項8之裝置，其中：

該通訊事件是一切換事件；以及

用於監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期的該監測邏輯包括：

比較邏輯，用於將該至少一個安全密鑰的一剩餘生存期與該切換事件的一預期持續時間進行比較。

11、根據請求項8之裝置，其中：

該通訊事件是一省電模式；以及

用於監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期的該監測邏輯包括：

比較邏輯，用於將該至少一個安全密鑰的一剩餘生存期與該省電模式的一低功率狀態的一時段進行比較。

12、根據請求項11之裝置，其中該省電模式包括一休眠模式。

13、根據請求項11之裝置，其中該省電模式包括一空閒模式。

14、根據請求項8之裝置，其中該裝置包括：

通訊邏輯，用於依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

15、一種維持一無線設備用於無線通訊的一或多個安全密鑰的裝置，包括：

確定構件，用於確定一通訊事件何時要發生；

監測構件，用於監測該一或多個安全密鑰的生存期，以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期；

延遲構件，用於：如果確定出該至少一個安全密鑰可能會到期，則延遲該通訊事件；以及

刷新構件，用於刷新所確定出的可能會到期的該至少一個安全密鑰。

16、根據請求項15之裝置，還包括：

重複執行構件，用於重複執行該確定構件、該監測構件、

該延遲構件、該刷新構件，直到確定出沒有任何安全密鑰可能會到期爲止；以及

通訊事件啓動構件，用於啓動該通訊事件。

17、根據請求項15之裝置，其中：

該通訊事件是一切換事件；以及

用於監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期的該監測構件包括：

比較構件，用於將該至少一個安全密鑰的一剩餘生存期與該切換事件的一預期持續時間進行比較。

18、根據請求項15之裝置，其中：

該通訊事件是一省電模式；以及

用於監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期的該監測構件包括：

比較構件，用於將該至少一個安全密鑰的一剩餘生存期與該省電模式的一低功率狀態的一時段進行比較。

19、根據請求項18之裝置，其中該省電模式包括一休眠模式。

20、根據請求項18之裝置，其中該省電模式包括一空閒

模式。

21、根據請求項15之裝置，其中該裝置包括：

通訊構件，用於依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

22、一種維持一無線設備用於無線通訊的一或多個安全密鑰的電腦程式產品，包括上面儲存有指令集的一電腦可讀取媒體，其中該指令集可由一或多個處理器來執行，該指令集包括：

確定指令，用於確定一通訊事件何時要發生；

監測指令，用於監測該一或多個安全密鑰的生存期，以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期；

延遲指令，用於：如果確定出該至少一個安全密鑰可能會到期，則延遲該通訊事件；以及

刷新指令，用於刷新所確定出的可能會到期的該至少一個安全密鑰。

23、根據請求項22之電腦程式產品，該指令集還包括：

重複執行指令，用於重複執行該確定指令、該監測指令、該延遲指令、該刷新指令，直到確定出沒有任何安全密鑰可能會到期爲止；以及

通訊事件啓動指令，用於啓動該通訊事件。

24、根據請求項22之電腦程式產品，其中：

該通訊事件是一切換事件；以及

用於監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期的該監測指令包括：

比較指令，用於將該至少一個安全密鑰的一剩餘生存期與該切換事件的一預期持續時間進行比較。

25、根據請求項22之電腦程式產品，其中：

該通訊事件是一省電模式；以及

用於監測該一或多個安全密鑰的生存期以確定是否有至少一個安全密鑰在該通訊事件期間可能會到期的該監測指令包括：

比較指令，用於將該至少一個安全密鑰的一剩餘生存期與該省電模式的一低功率狀態的一時段進行比較。

26、根據請求項25之電腦程式產品，其中該省電模式包括一休眠模式。

27、根據請求項25之電腦程式產品，其中該省電模式包括一空閒模式。

28、根據請求項22之電腦程式產品，其中該指令集包括：

通訊指令，用於依據電氣與電子工程師協會（IEEE）802.16標準族的一項或多項標準，使用訊框來進行通訊。

200952425

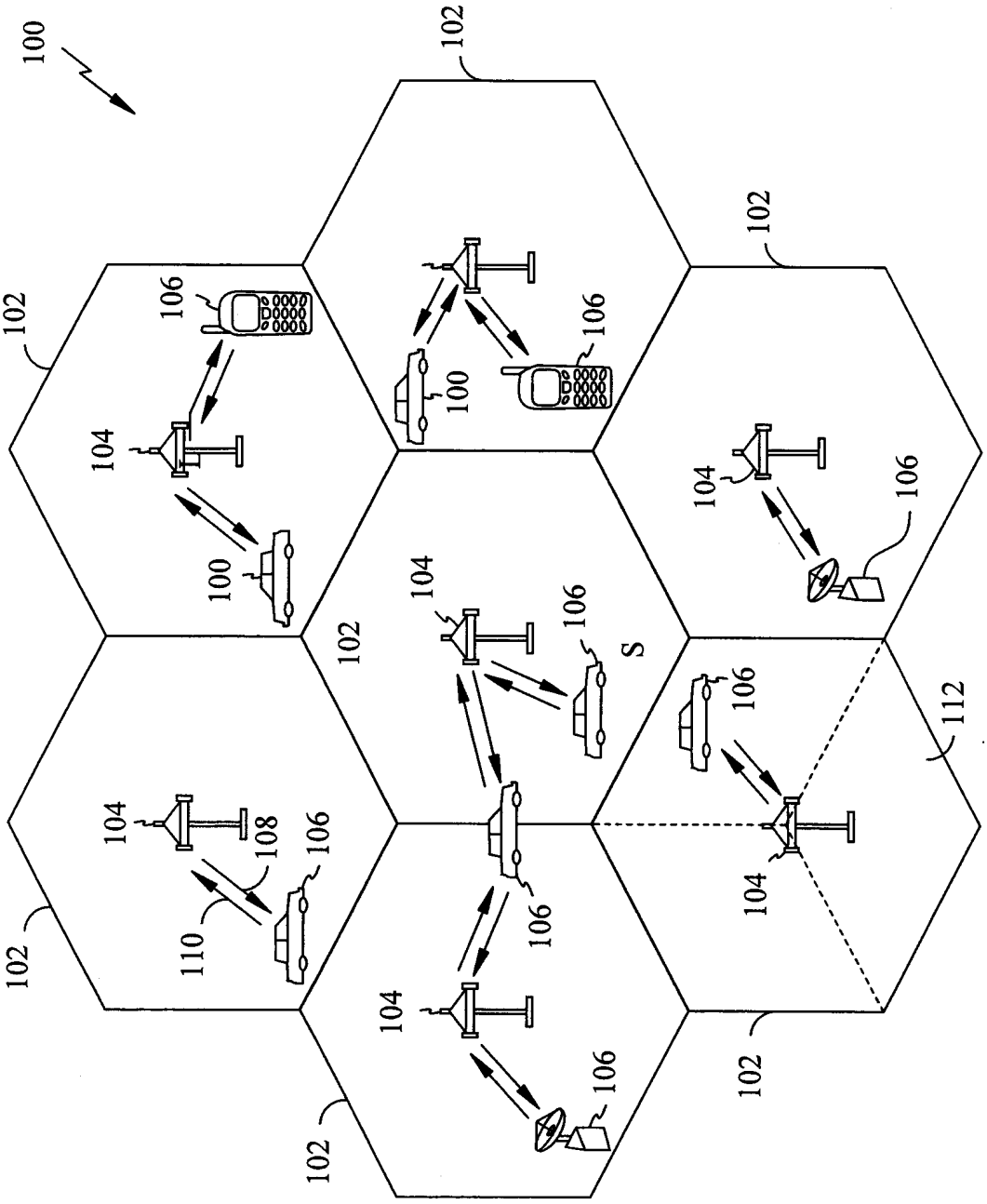


圖 1

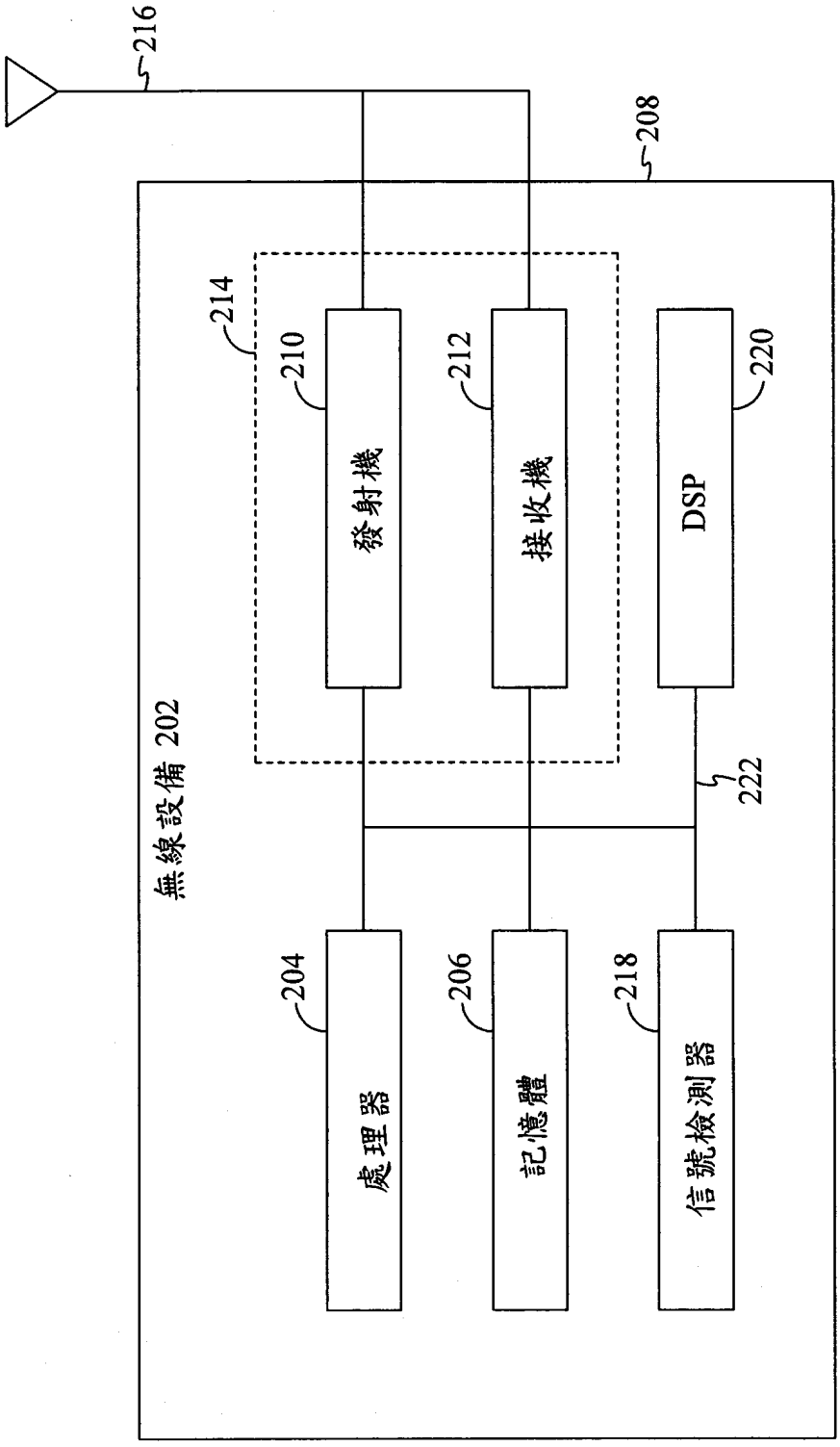

216
208
214
210
發射機
212
接收機
220
DSP
無線設備 202
222
204
處理器
206
記憶體
218
信號檢測器

圖2

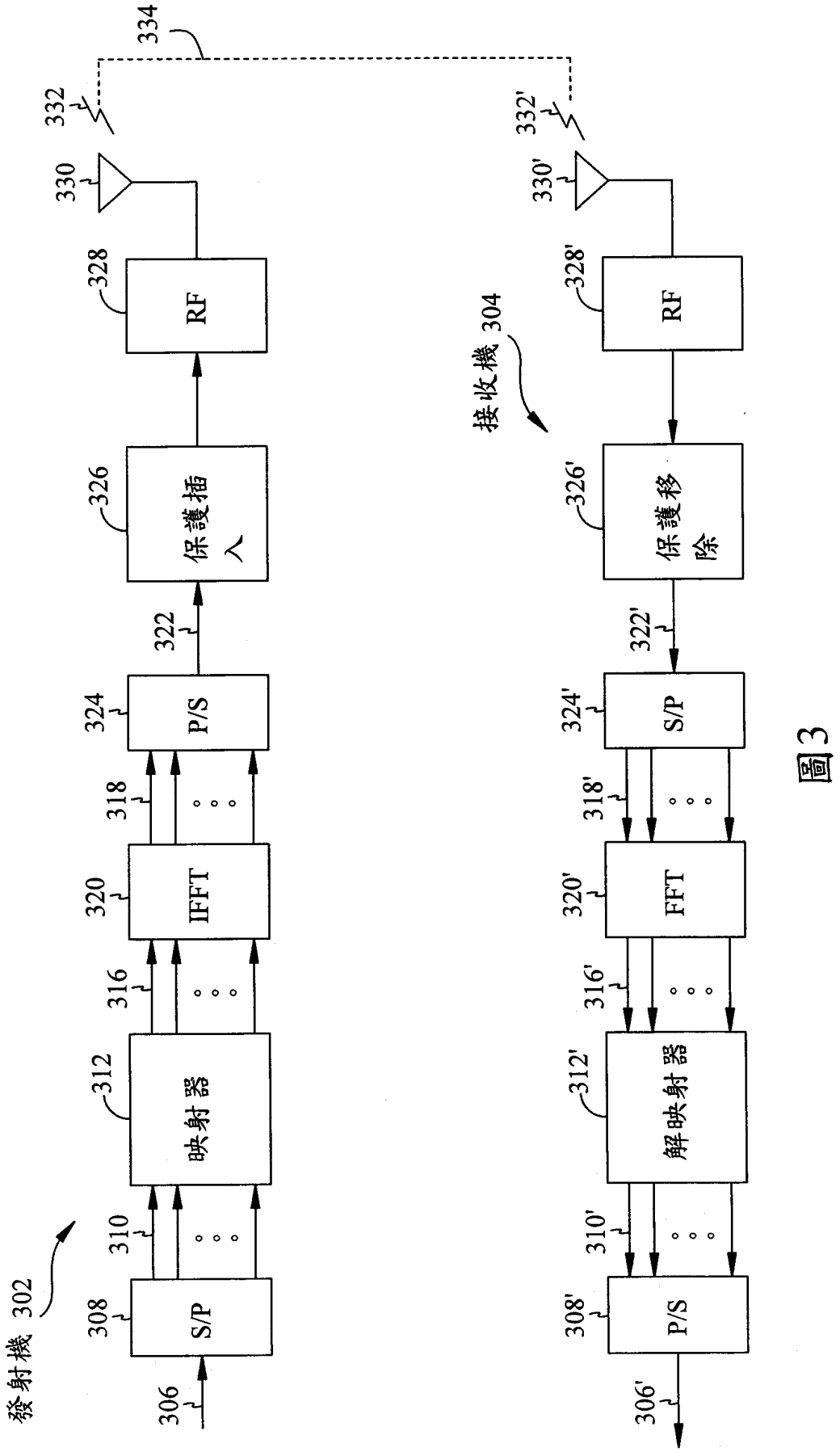

發射機 302
306
S/P
308
310
映射器
312
316
IFFT
320
318
P/S
324
322
保護插入
326
RF
328
330
332
334
接收機 304
306'
P/S
308'
310'
解映射器
312'
316'
FFT
320'
318'
S/P
324'
322'
保護移除
326'
RF
328'
330'
332'

圖3

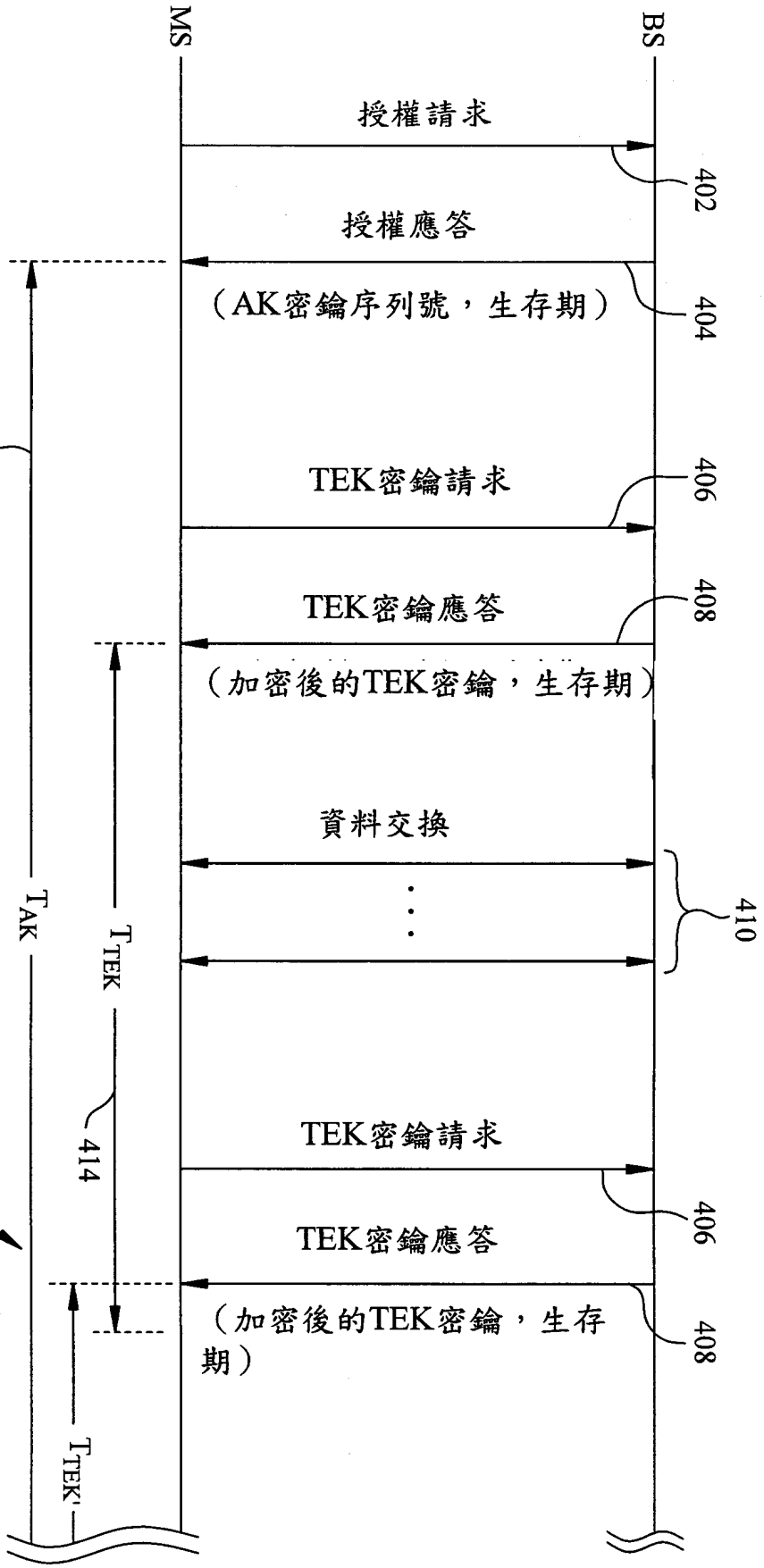

MS
BS
授權請求
402
授權應答
（AK密鑰序列號，生存期）
404
412
TEK密鑰請求
406
TEK密鑰應答
408
（加密後的TEK密鑰，生存期）
資料交換
410
TEK密鑰請求
406
TEK密鑰應答
（加密後的TEK密鑰，生存期）
408
414
T_{AK}
T_{TEK}
$T_{TEK'}$
在生存期屆滿之前刷新TEK密鑰

圖4

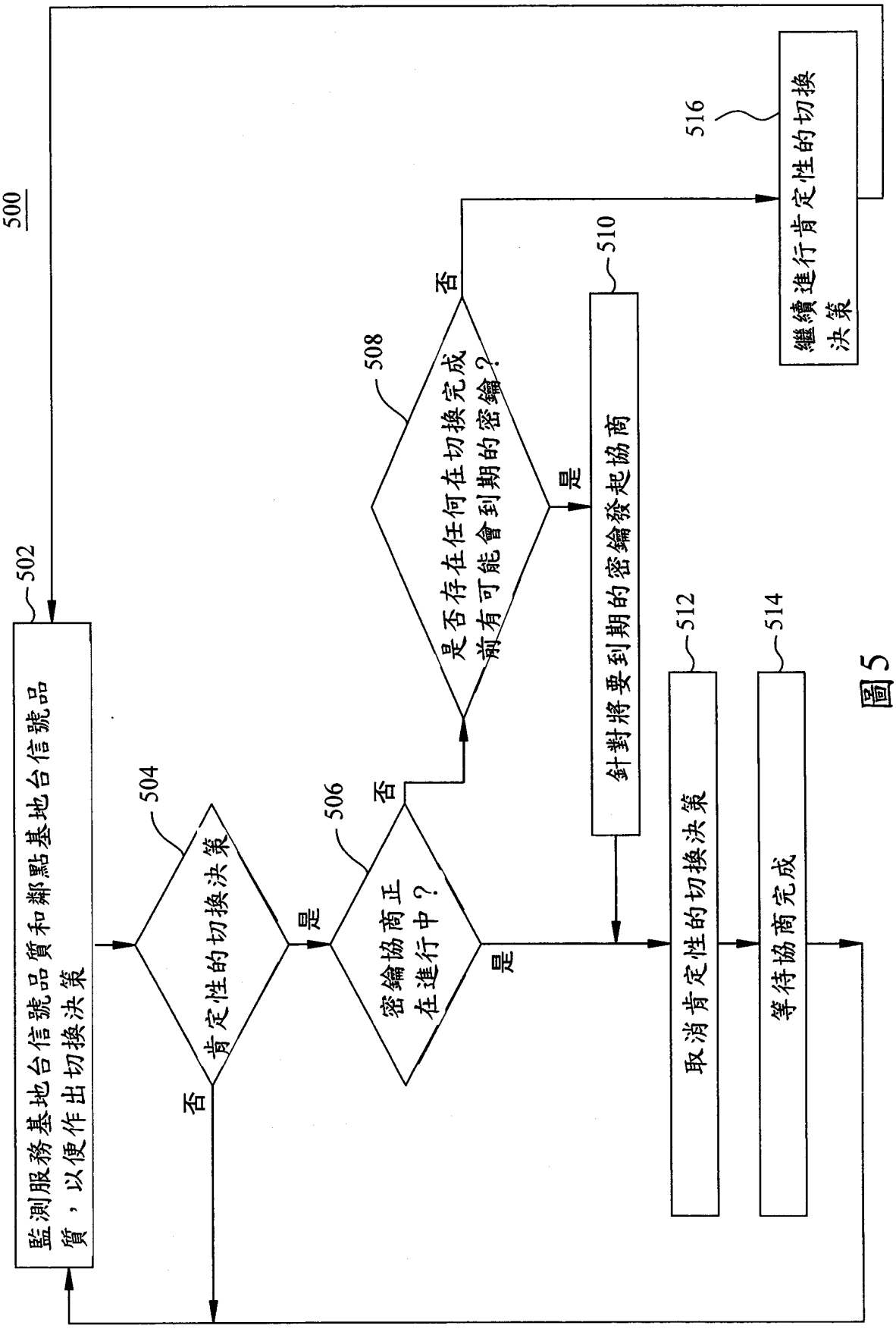

500
502
監測服務基地台信號品質和鄰點基地台信號品質，以便作出切換決策
504
肯定性的切換決策
否
是
506
密鑰協商正在進行中？
否
是
508
是否存在任何在切換完成前有可能會到期的密鑰？
否
是
510
針對將要到期的密鑰發起協商
512
取消肯定性的切換決策
514
等待協商完成
516
繼續進行肯定性的切換決策

圖 5

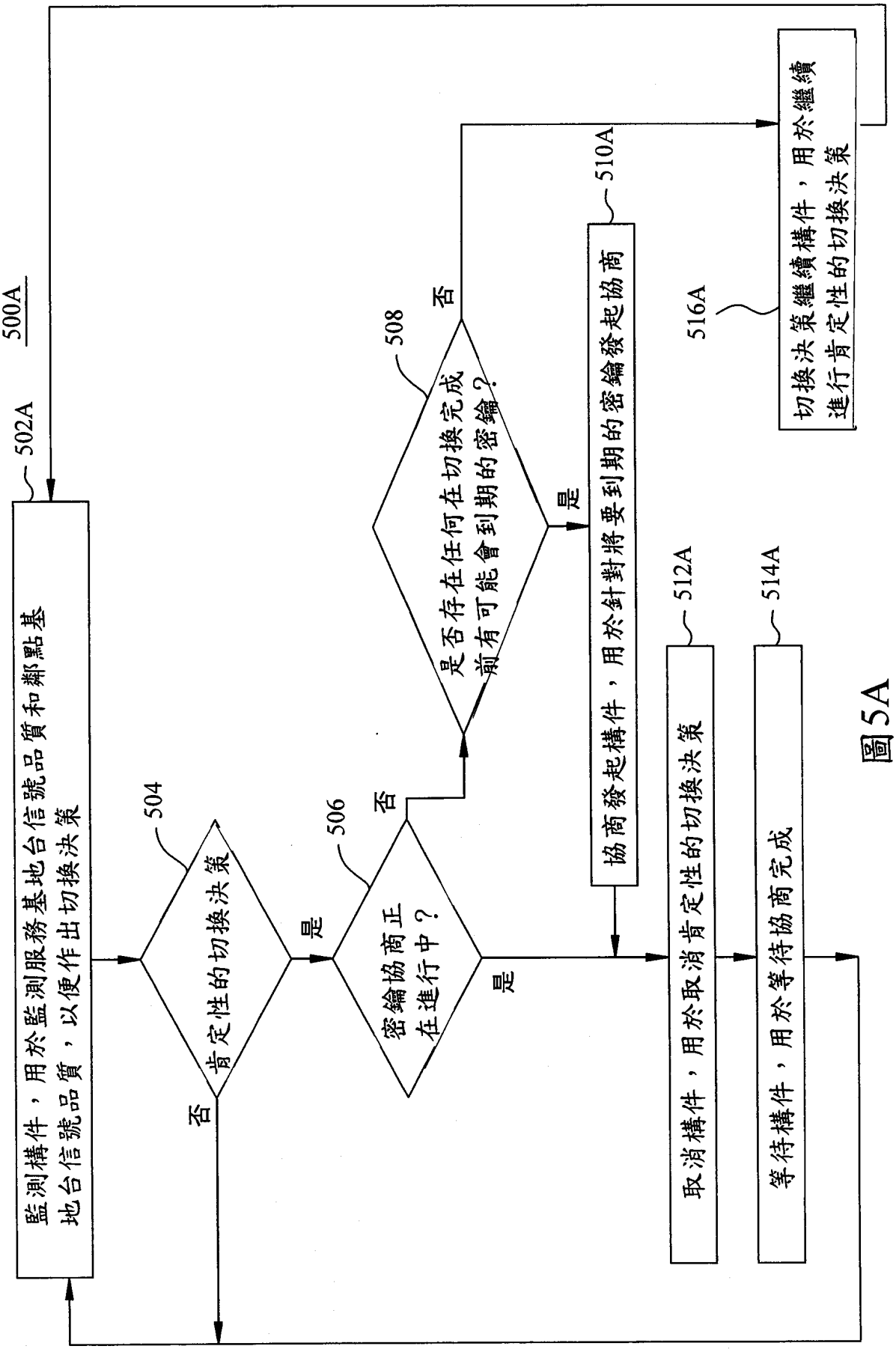

500A
502A
監測構件，用於監測服務基地台信號品質和鄰點基地台信號品質，以便作出切換決策
504
肯定性的切換決策
否
是
506
密鑰協商正在進行中？
否
是
508
是否存在任何在切換完成前有可能會到期的密鑰？
否
是
510A
協商發起構件，用於針對將要到期的密鑰發起協商
512A
取消構件，用於取消肯定性的切換決策
514A
等待構件，用於等待協商完成
516A
切換決策繼續構件，用於繼續進行肯定性的切換決策

圖5A

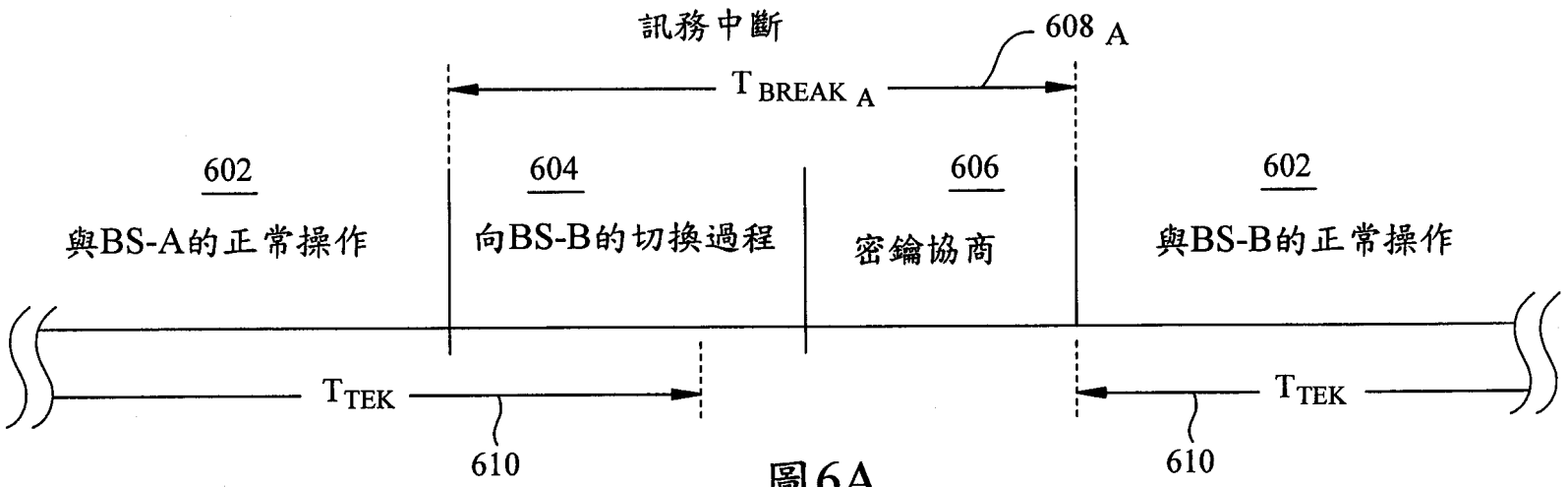

訊務中斷
608 A
T BREAK A
602
與BS-A的正常操作
604
向BS-B的切換過程
606
密鑰協商
602
與BS-B的正常操作
T TEK
610
T TEK
610

圖6A

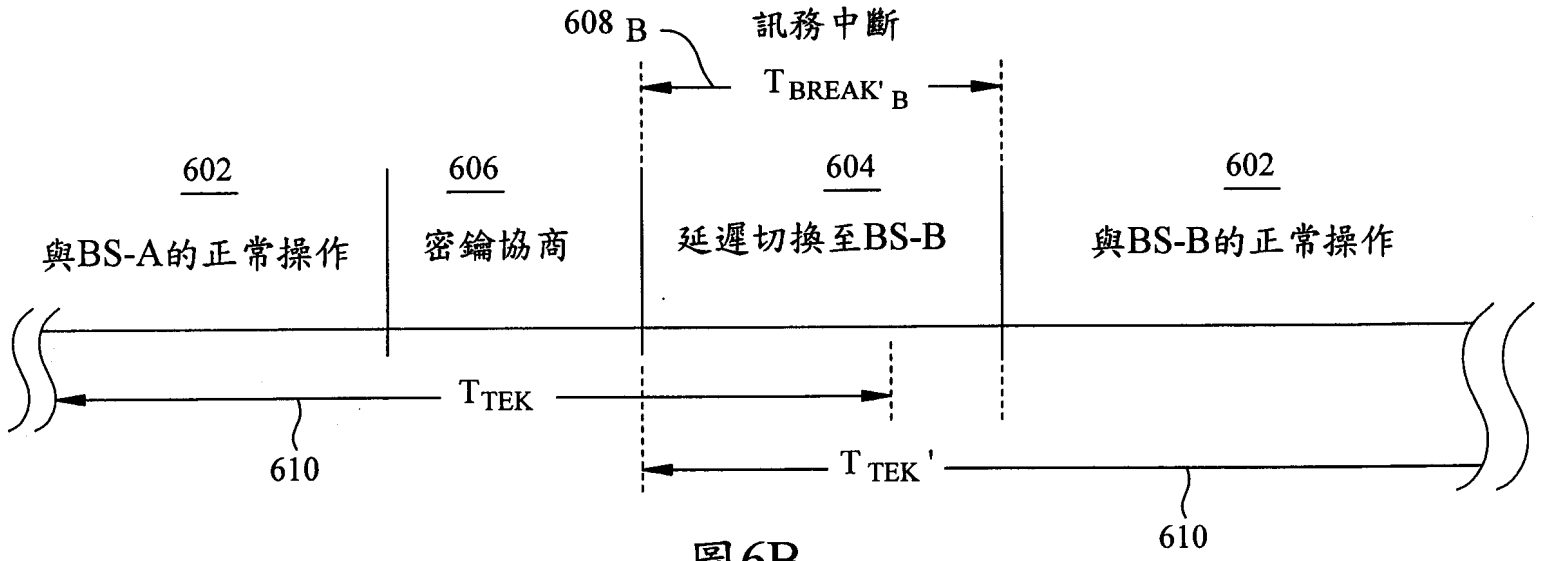

608 B
訊務中斷
T BREAK' B
602
與BS-A的正常操作
606
密鑰協商
604
延遲切換至BS-B
602
與BS-B的正常操作
T TEK
610
T TEK '
610

圖6B

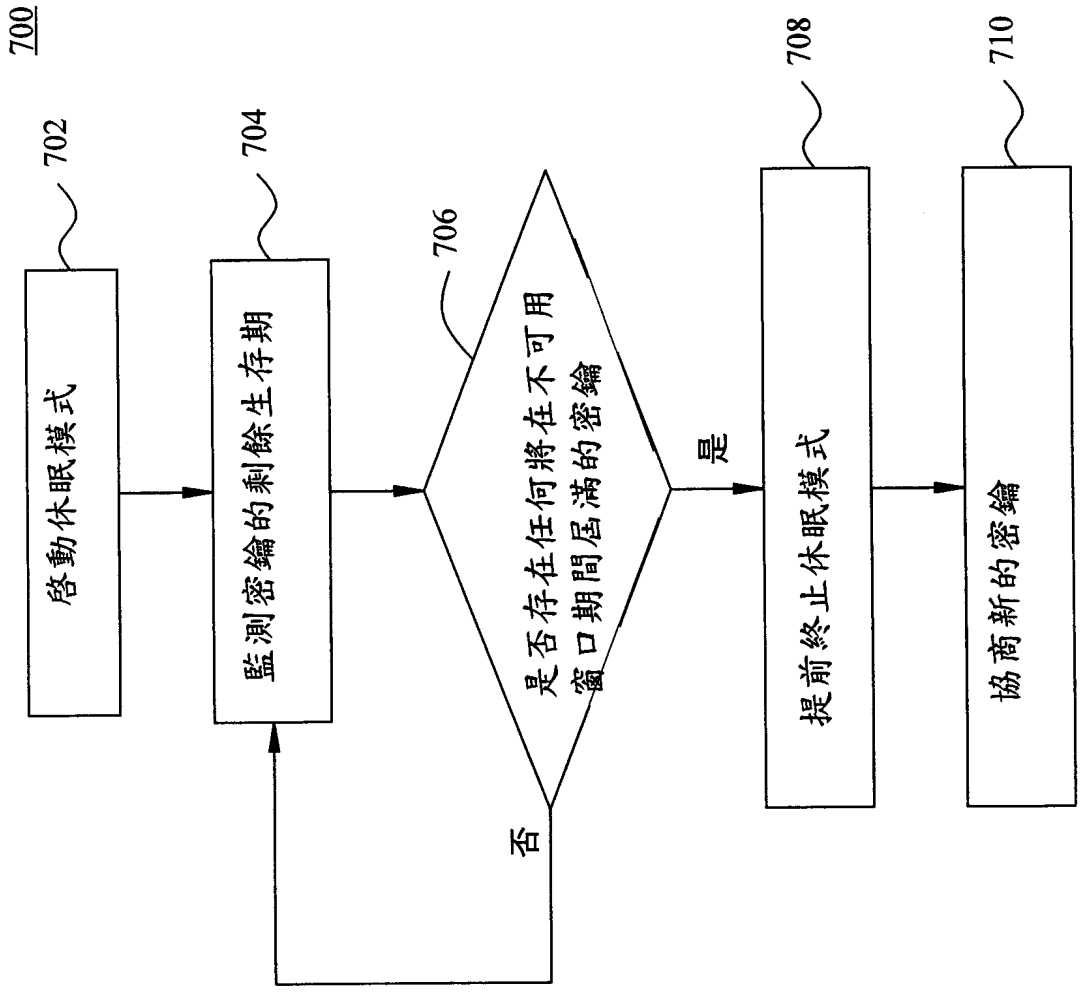

700
702
啓動休眠模式
704
監測密鑰的剩餘生存期
706
是否存在任何將在不可用窗口期間屆滿的密鑰
是
否
708
提前終止休眠模式
710
協商新的密鑰

圖7

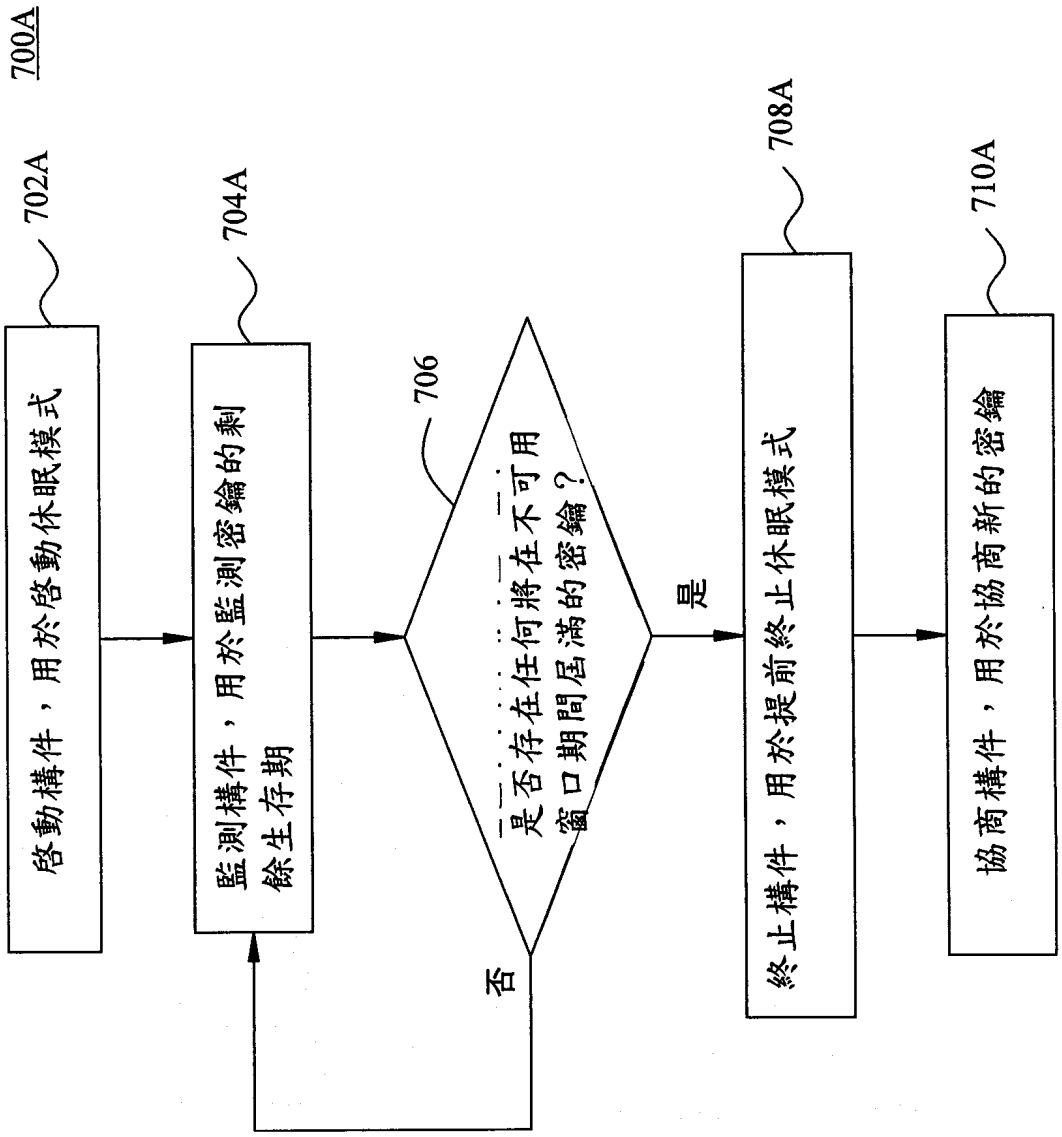

700A
702A
啓動構件，用於啓動休眠模式
704A
監測構件，用於監測密鑰的剩餘生存期
706
是否存在任何將在不可用窗口期間屆滿的密鑰？
否
是
708A
終止構件，用於提前終止休眠模式
710A
協商構件，用於協商新的密鑰

圖7A

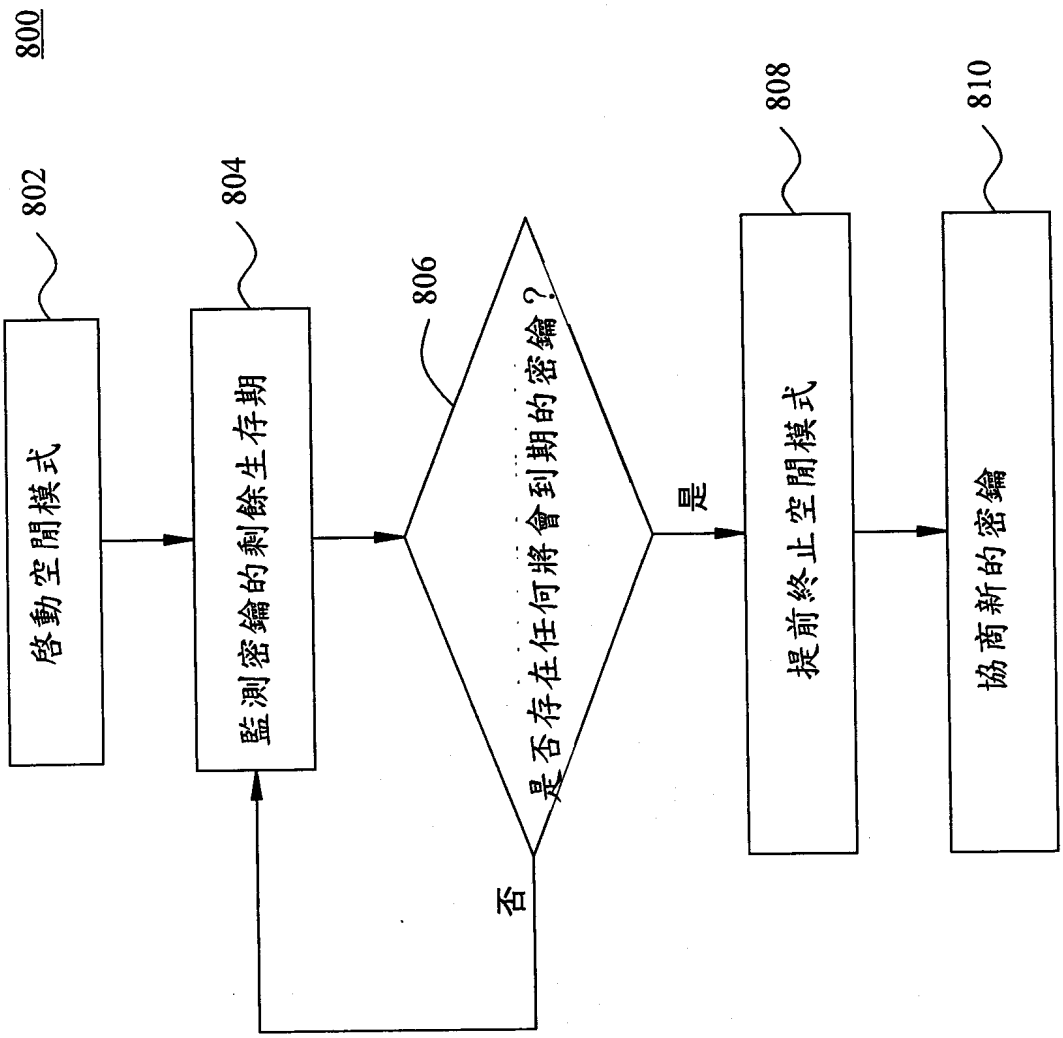

800
802
啓動空閒模式
804
監測密鑰的剩餘生存期
806
是否存在任何將會到期的密鑰？
是
否
808
提前終止空閒模式
810
協商新的密鑰

圖8

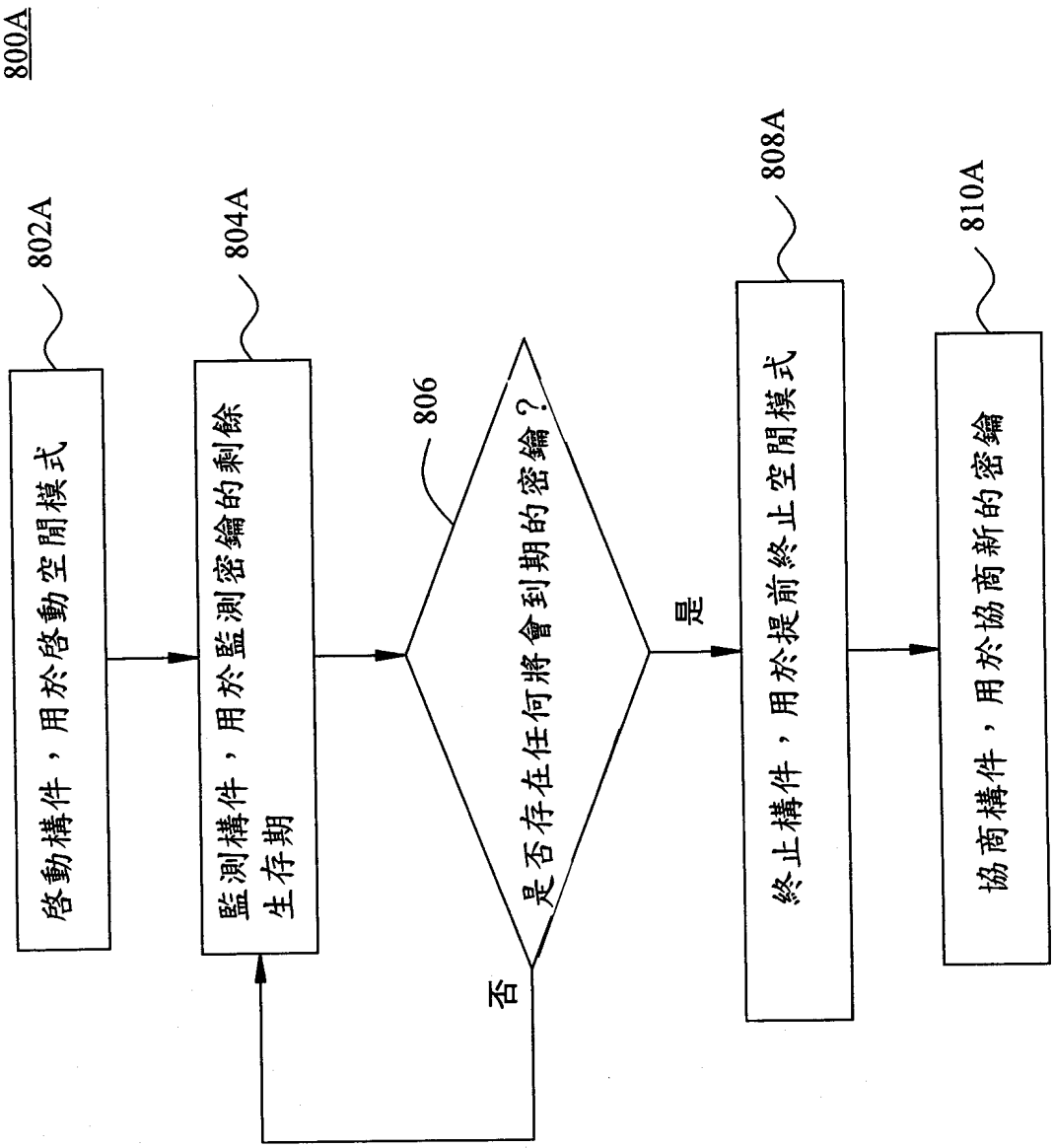

800A
802A
啓動構件，用於啓動空閒模式
804A
監測構件，用於監測密鑰的剩餘生存期
806
是否存在任何將會到期的密鑰？
否
是
808A
終止構件，用於提前終止空閒模式
810A
協商構件，用於協商新的密鑰

圖8A

四、指定代表圖：

(一)本案指定代表圖為：第（ 5 ）圖。

(二)本代表圖之元件符號簡單說明:

無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無