201018165

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：97140881

※ 申請日期：97.10.24　※IPC 分類：H04L 9/00 (2006.01)

一、發明名稱：（中文/英文）

金鑰更新裝置、方法及其電腦程式產品及包含前述裝置之無線網路系統

APPARATUS AND METHOD FOR RENEWING A KEY, COMPUTER PROGRAM PRODUCT THEREOF AND WIRELESS NETWORK SYSTEM COMPRISING THE SAME

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

財團法人資訊工業策進會

INSTITUTE FOR INFORMATION INDUSTRY

代表人：（中文/英文）　陳瑞隆/CHEN, RUEY-LONG

住居所或營業所地址：（中文/英文）

台北市和平東路二段 106 號 11 樓

11 FL., NO. 106, SEC. 2, HO-PING E. RD., TAIPEI, TAIWAN, R.O.C.

國　籍：（中文/英文）　中華民國/TAIWAN, R.O.C.

三、發明人：（共 7 人）

姓　名：（中文/英文）

蔡其達/TSAI, FRANK CHEE-DA

邱簡謙/CHIU, CHIEN-CHIEN

林益宏/LIN, I-HUNG

孫宏民/SUN, HUNG-MIN

張仕穎/CHANG, SHIH-YING

邢傑/HSING, CHIEH

高啟益/KAO, CHI-YI

國　籍：(中文/英文)

中華民國/TAIWAN, 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】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 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。

邢傑/HSING, CHIEH

高啟益/KAO, CHI-YI

國　籍：(中文/英文)

中華民國/TAIWAN, 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】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 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。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種金鑰更新裝置、方法、其電腦程式產品及包含前述金鑰更新裝置之無線網路系統；更詳細地說，本發明係關於一種減少即時更新金鑰次數之金鑰更新裝置、方法、其電腦程式產品及包含前述金鑰更新裝置之無線網路系統。

【先前技術】

近年來，隨著時代的進步，人們使用行動裝置進行溝通的時間也日益增加。目前的行動裝置大都有其專屬的無線網路系統，例如全球行動通訊系統（Global System for Mobile Communications；GSM）、寬頻多碼分工（Wideband Code Division Multiple Access；WCDMA）、全球互通微波存取（Worldwide Interoperability for Microwave Access；WiMax）等等。該些無線網路系統皆提供群播（multicast）之功能，以滿足某些特定用戶的個別需求。透過群播傳送訊息時，必須使用一金鑰。於此群組內的行動裝置皆能使用此金鑰解密訊息，而不在此群組內的行動裝置因不具有此金鑰，因此即便取得訊息，亦無法對其進行解密。

由於大部分的無線網路系統都由複數個基地台組成，因此當屬於特定群組之行動裝置在各基地台之訊號範圍間移動時，各基地台如何管理群組金鑰為相當重要的課題。習知技術係使每一基地台使用一金鑰，但當有行動裝置進入基地台之訊號範圍時，基地台必須更新金鑰再將更新後之金鑰傳送給此群組之所有行動裝置。此外，當有行動裝置離開基地台之訊號範圍時，基地台亦會更新金鑰，在傳送更新後之金鑰給此群組之所有行動裝置。當行

動裝置數量超過一定數量時，無線網路系統對予各該行動裝置的更新金鑰的動作也更趨頻繁，造成過大的成本。

綜上所述，如何降低無線網路系統更新金鑰之成本為此領域亟需解決的問題。

【發明內容】

本發明之一目的在於提供一種金鑰更新方法。該金鑰更新方法適用於一第一基地台，該第一基地台屬於一無線網路系統。該第一基地台具有一第一訊號範圍且使用一第一金鑰。該金鑰更新方法包含下列步驟：判斷一行動裝置由一第二基地台所具有之一第二訊號範圍進入該第一訊號範圍，其中該第一訊號範圍與該第二訊號範圍部分重疊，該第二基地台屬於該無線網路系統，且該第二基地台使用一第二金鑰；判斷該行動裝置登入該無線網路系統之一登入時間晚於該第一金鑰之一更新時間；因應該登入時間晚於該第一金鑰之該更新時間之判斷結果，更新該第一金鑰；以及傳送該第一金鑰予該行動裝置。

本發明之另一目的在於提供一種金鑰更新裝置。該金鑰更新裝置，適用於一第一基地台，該第一基地台具有一第一訊號範圍，且該第一基地台屬於一無線網路系統。該金鑰更新裝置包含一儲存模組、一處理模組及一傳送模組。該儲存模組用以儲存該第一基地台使用之一第一金鑰。該處理模組用以判斷一行動裝置由一第二基地台之一第二訊號範圍進入該第一訊號範圍，用以判斷該行動裝置登入該無線網路之一登入時間晚於該第一金鑰之一更新時間，以及用以因應該登入時間晚於該第一金鑰之該更新時間之判斷結果，更新該第一金鑰。其中該第一訊號範圍與該第二訊號

範圍部分重疊，該第二基地台屬於該無線網路，且該第二基地台使用一第二金鑰。該傳送模組則用以傳送該第一金鑰予該行動裝置。

本發明之另一目的在於提供一種電腦程式產品，內儲一種用以進行金鑰更新之程式。該電腦程式產品適用於一第一基地台，該第一基地台屬於一無線網路，且該第一基地台使用一第一金鑰。該程式被載入該第一基地台之一微處理器後執行程式指令A、B、C及D。程式指令A使該微處理器判斷一行動裝置由一第二基地台之一第二訊號範圍進入該第一訊號範圍，其中該第一訊號範圍與該第二訊號範圍部分重疊，該第二基地台屬於該無線網路，且該第二基地台使用一第二金鑰。程式指令B使該微處理器判斷該行動裝置登入該無線網路之一登入時間晚於該第一金鑰之一更新時間。程式指令C使該微處理器於執行該程式指令B後，更新該第一金鑰。程式指令D使該微處理器傳送該第一金鑰予該行動裝置。

具體而言，本發明所揭露之技術，於行動裝置由第二基地台之第二訊號範圍移動至第一基地台之第一訊號範圍時，第一基地台會判斷是否需要更新其所使用之第一金鑰。若行動裝置登入無線網路系統之時間晚於第一基地台之第一金鑰之更新時間，則第一基地台立即更新第一金鑰，否則便不更新，藉此可降低無線網路系統更新金鑰之次數。

在參閱圖式及隨後描述之實施方式後，該技術領域具有通常知識者便可瞭解本發明之其他目的，以及本發明之技術手段及實施

態樣。

【實施方式】

以下將透過實施例來解釋本發明內容，本發明之描述係關於一種金鑰更新方法、裝置及使用前述方法及裝置之無線網路系統。本發明將更新金鑰的時間點區分為即時的更新時間點及非即時的更新時間點。於非即時的更新時間點之金鑰更新動作將被延遲至之後的即時的更新時間點批次處理，以降低無線網路系統 1 更新金鑰所造成之負擔。本發明之實施例並不侷限於特定的環境、應用或實施，因此，以下實施例之描述僅為說明目的，並非本發明之限制。

本發明之第一實施例為一無線網路系統 1，其示意圖如第 1 圖所描繪。無線網路系統 1 包含一第一基地台 107 及一第二基地台 103，其中第一基地台 107 具有一第一訊號範圍 109，第二基地台 103 具有一第二訊號範圍 105，且第一訊號範圍 109 與第二訊號範圍 105 部份重疊。第一基地台 107 使用一第一金鑰以加密其所要傳送之訊息，因此於第一訊號範圍 109 內之行動裝置需取得第一金鑰才能解密第一基地台 107 所傳送的訊息，而已離開第一訊號範圍 109 之行動裝置則不能取得現在使用的第一金鑰。同理，第二基地台 103 使用一第二金鑰加密其所要傳之訊息，因此第二訊號範圍 105 內之行動裝置須取得第二金鑰才能解密第二基地台 103 所傳送的訊息，而已離開第二訊號範圍 105 之行動裝置則不能取得現在使用的第二金鑰。

需說明者，第一實施例中，「第一」及「第二」僅用來表達為二個不同的基地台、各基地台之訊號範圍及各基地台所使用之金

鑰，並無其他涵義。

第一基地台 107 及第二基地台 103 分別設置一金鑰更新裝置 201a、201b。第 2 圖描繪金鑰更新裝置 201a、201b 之示意圖，金鑰更新裝置 201a、201b 包含一儲存模組 203a、203b、一處理模組 205a、205b 及一傳送模組 207a、207b。第一基地台 107 之儲存模組 203a 儲存第一金鑰，且第二基地台 103 之儲存模組 203b 儲存第二金鑰。

接著說明第一基地台 107 之金鑰更新裝置 201a 如何適時更新第一金鑰及第二基地台 103 之金鑰更新裝置 201b 如何適時更新第二金鑰。

於早上九點，行動裝置 113 由位置 E 進入第一基地台 107 之第一訊號範圍 109。此時，第一基地台 107 之處理模組 205a 判斷行動裝置 113 於早上九點之前並未進入第一訊號範圍 109 或第二訊號範圍 105，故認定行動裝置 113 於此時登入無線網路系統 1。在第一基地台 107 中，行動裝置登入無線網路系統 1 之時間點被設定為即時的更新時間點，因此第一基地台 107 之處理模組 205a 更新第一金鑰。儲存模組 203a 則儲存更新後的第一金鑰（早上九點更新），此外，傳送模組 207a 傳送更新後的第一金鑰（早上九點更新）予行動裝置 113。另一方面，行動裝置 113 記錄自己登錄無線網路系統 1 之一登入時間為早上九點，而儲存模組 203a 記錄行動裝置 113 進入第一訊號範圍 109。

之後，於早上九點二十分時，行動裝置 111 由位置 A 進入第二基地台 103 之第二訊號範圍 105。此時第二基地台 103 之處理模組

205b 判斷行動裝置 111 於早上九點二十分之前並未進入第一訊號範圍 109 或第二訊號範圍 105，故認定行動裝置 111 於此時登入無線網路系統 1。在第二基地台 103 中，行動裝置登入無線網路系統 1 之時間點被設定為即時的更新時間點，因此第二基地台 103 之處理模組 205b 更新第二金鑰。儲存模組 203b 儲存更新後之第二金鑰（早上九點二十分更新），且傳送裝置 207b 傳送此更新後之第二金鑰（早上九點二十分更新）予行動裝置 111。另一方面，行動裝置 111 記錄自己登錄無線網路系統 1 之一登入時間為早上九點二十分，且儲存模組 203b 記錄行動裝置 111 進入第二訊號範圍 105。

接著，於早上九點三十分，行動裝置 113 移動至位置 F。此時，第二基地台 103 之處理模組 205b 判斷行動裝置 113 由第一訊號範圍 109 進入第二訊號範圍 105。接著，第二基地台 103 之處理模組 205b 判斷行動裝置 113 登入無線網路系統 1 之登入時間（早上九點）早於第二金鑰之更新時間（早上九點二十分）。於第二基地台中 103，當行動裝置登入無線網路系統之登入時間早於第二金鑰之更新時間時，為非即時的更新時間點，因此處理模組 205b 不更新第二金鑰。之後，第二基地台 103 之傳送模組 207b 傳送第二金鑰（早上九點二十分更新）予行動裝置 113。另一方面，由於行動裝置 113 已離開第一基地台 107 之第一訊號範圍 109，因此第一基地台 107 之儲存模組 203a 記錄行動裝置 113 已離開第一訊號範圍 109 且曾取得第一金鑰。

於早上九點五十分，行動裝置 111 移動至位置 B。此時，第一基

地台 107 之處理模組 205a 判斷行動裝置 111 由第二基地台 103 之第二訊號範圍 105 進入第一基地台 107 之第一訊號範圍 109。接著，第一基地台 107 之處理模組 205a 判斷行動裝置 111 登入無線網路系統 1 之登入時間（早上九點二十分）晚於第一金鑰之更新時間（早上九點）。於第一基地台 107 中，當行動裝置登入無線網路系統之登入時間晚於第一金鑰之更新時間時，為即時的更新時間點，因此處理模組 205a 因應此判斷結果，立即更新第一金鑰。儲存模組 203a 則儲存更新後之第一金鑰（早上九點五十更新），而傳送模組 207a 傳送第一金鑰（早上九點五十更新）予行動裝置 111。另一方面，由於行動裝置 111 已離開第二基地台 103 之第二訊號範圍 105，因此第二基地台 103 之儲存模組 203b 記錄行動裝置 111 已離開第二訊號範圍 105 且曾取得第二金鑰。

接著，於早上十點，行動裝置 113 移動至位置 H。第二基地台 103 之處理模組 205b 判斷行動裝置 113 離開第二訊號範圍 105，且判斷行動裝置 113 係由第二基地台 103 登出無線網路系統 1。此時，儲存模組 203b 記錄行動裝置 113 離開第二訊號範圍 105 且曾取得第二金鑰。

接著，處理模組 205a 判斷第一基地台 107 於行動裝置 113 離開第一訊號範圍 109 後，第一基地台 107 是否更新過第一金鑰。第一基地台中，若前述的判斷為行動裝置 113 離開第一訊號範圍 109 後，第一基地台 107 未更新過第一金鑰，則此時間點為即時的更新時間點。由於行動裝置 113 係於早上九點三十分離開第一訊號範圍，而第一金鑰於早上九點五十分被更新過，因此第一基地台

107之處理模組205a不更新第一金鑰。

另一方面，處理模組205b判斷第二基地台103於行動裝置113離開第二訊號範圍105後，是否更新過第二金鑰。第二基地台中，若前述的判斷為行動裝置113離開第二訊號範圍105後，第二基地台103未曾更新第二金鑰，則此時間點為即時的更新時間點。由於行動裝置113於早上十點離開第二訊號範圍105，而第二金鑰之前於早上九點二十分被更新，因此第二基地台103之處理模組205b更新第二金鑰。第二基地台103之儲存模組203b則儲存更新過之第二金鑰（十點更新）。

於早上十點二十分，行動裝置111移動至位置D。第一基地台107之處理模組205a判斷行動裝置111離開第一訊號範圍109，且判斷行動裝置111由第一基地台107登出無線網路系統101。此時，儲存模組203a記錄行動裝置111離開第一訊號範圍109且曾取得第一金鑰。

接著，第一基地台107之處理模組205a判斷於行動裝置111離開第一訊號範圍109後，第一基地台103是否更新過第一金鑰。由於行動裝置111係於早上十點二十分離開第一訊號範圍109，而第一金鑰之前於早上九點五十分被更新，表示行動裝置111離開第一訊號範圍109後，第一基地台103未曾更新第一金鑰，因此第一基地台107之處理模組205a更新第一金鑰。儲存模組203a則儲存更新後之第一金鑰（十點二十分更新）。

另一方面，處理模組205a判斷第二基地台103於行動裝置111離開第二訊號範圍105後，是否更新過第二金鑰。由於行動裝置

111 係於早上九點五十分離開第二訊號範圍 105，而第二金鑰之前於早上十點被更新。由於第二基地台 103 於行動裝置 111 離開第二訊號範圍 105 後曾更新第二金鑰，因此第二基地台 103 之處理模組 205b 此時不更新第二金鑰。

第一實施例中，行動裝置 113 從登入至登出無線網路系統 1 之時間內，無線網路系統 1 內共進行了二次的金鑰更新。行動裝置 111 從登入至登出網路系統 1 之時間內，無線網路系統 1 內共進行了三次的金鑰更新。若採用習知技術（即當行動裝置進入及離開一基地台之訊號範圍皆需更新金鑰），則行動裝置 113 從登入至登出無線網路系統 1 之時間內需進行四次金鑰更新，行動裝置 111 之情形亦然。由此數字可知，第一實施例大幅減少金鑰更新之次數。

由上述說明可知，第一實施例中，屬於無線網路系統 1 之所有基地台（即第一基地台 107 及第二基地台 103）皆將更新金鑰的時間點區分為即時的更新時間點及非即時的更新時間點。具體來說，當一行動裝置經由一目標基地台（可為第一基地台 107 或第二基地台 103）登入無線網路系統 1 時，此時間點為即時的更新時間點，因此目標基地台即時更新其所使用之金鑰（可為第一金鑰或第二金鑰）。

另一方面，當行動裝置由一原始基地台之訊號範圍進入一目標基地台之訊號範圍（例如由第一基地台 107 之第一訊號範圍 109 進入第二基地台 103 之第二訊號範圍 105，或由第二基地台 103 之第二訊號範圍 105 進入第一基地台 107 之第一訊號範圍 109）時

間點，目標基地台未必需要立即更新其所使用的金鑰。詳言之，目標基地台會比較自己所使用之金鑰之最新的更新時間與行動裝置登入無線網路系統 1 之登入時間，以判斷此時間點為即時的更新時間點或非即時的更新時間點。若行動裝置登入無線網路系統 1 之登入時間較晚，則為即時的更新時間點，目標基地台需立即更新其所使用的金鑰。反之（行動裝置登入無線網路系統 1 之登入時間較早），則為非即時的更新時間點，故此時不需更新金鑰。

當行動裝置登出無線網路系統 1 時，各個基地台（即第一基地台 107 及第二基地台 103）需判斷當行動裝置離開其訊號範圍後，是否曾經更新過金鑰，若未曾更新，則於這個時間點必須更新金鑰。

要特別強調的是，無線網路系統 1 並不限制基地台之數目。若無線網路系統 1 更包含其他的基地台，則這些基地台亦採用同樣的判斷方式。因此，不論無線網路系統 1 包含多少個基地台，皆能降低金鑰交換之次數。

本發明之第二實施例為一種金鑰更新方法，其流程圖係描繪於第 3A 圖。與第一實施例相同，第二實施例亦將更新金鑰的時間點區分為即時的更新時間點及非即時的更新時間點。若為非即時之更新時間點，則將於後續即時的更新時間點再批次處理，藉此降低無線網路系統之負擔。

第二實施例之金鑰更新方法適用於一無線網路系統之所有基地台。為方便說明起見，第二實施例將以二個基地台為例進行說明，然而，須知基地台之數目並非用來限制本發明之範圍。第二實施

例之二個基地台稱為第一基地台及第二基地台，第一基地台具有一第一訊號範圍，且第二基地台具有一第二訊號範圍，其中，第一訊號範圍與第二訊號範圍部分重疊。第一基地台使用一第一金鑰，且第二基地台使用一第二金鑰。第二實施例中，「第一」及「第二」僅用來表達為二個不同的基地台、各基地台之訊號範圍及各基地台所使用之金鑰，並無其他涵義。以下以第一基地台為中心闡述第二實施例之金鑰更新方法，然於實際運作時，第二基地台亦採用同樣之金鑰更新方法。

首先執行步驟 301，第一基地台判斷是否有一行動裝置由第一基地台登入無線網路系統。若判斷結果為是，則第一基地台執行步驟 303 以更新第一金鑰，再執行步驟 305 以儲存更新後之第一金鑰。第一基地台更執行步驟 307，傳送更新後之第一金鑰予行動裝置。之後則進入步驟 309，結束金鑰更新方法。

若步驟 301 之判斷結果為否，則第一基地台執行步驟 311，判斷是否有一行動裝置由第一基地台登出無線網路系統。若步驟 311 之判斷結果為否，表示第一基地台判斷有一行動裝置由第二基地台之第二訊號範圍進入第一基地台之第一訊號範圍。接著，第二基地台執行步驟 313 以記錄行動裝置離開第二訊號範圍，第一基地台執行步驟 315 以記錄行動裝置進入第一訊號範圍。

第一基地台接著執行步驟 317，判斷行動裝置登入此無線網路系統之登入時間是否晚於第一金鑰之更新時間。若步驟 317 之判斷結果為行動裝置登入之時間較晚，則第一基地台執行步驟 303 以更新第一金鑰，再執行步驟 305 以儲存第一金鑰。第一基地台更

執行步驟 307 以傳送第一金鑰予行動裝置。之後則進入步驟 309，結束金鑰更新方法。若步驟 317 之判斷結果為行動裝置之登入時間不晚於第一金鑰之更新時間，則第一基地台直接執行步驟 307，傳送第一金鑰予行動裝置。之後則進入步驟 309，結束金鑰更新方法。

若步驟 311 之結果為是，表示第一基地台判斷行動裝置離開第一訊號範圍，且登出無線網路系統。第 3B 圖係描繪後續之流程圖。第一基地台執行步驟 319 以記錄行動裝置離開第一訊號範圍且行動裝置曾取得第一金鑰。之後第一基地台執行步驟 321，判斷行動裝置離開第一訊號範圍後，第一基地台是否更新過第一金鑰。若判斷之結果為否，則執行步驟 323 更新第一新鑰，再執行步驟 325 儲存更新後之第一金鑰。之後第二基地台執行步驟 327。若步驟 321 之結果為是，則第二基地台直接執行步驟 327。

步驟 327 係由第二基地台判斷行動裝置離開第二訊號範圍後，第二基地台是否更新過第二金鑰。若判斷之結果為否，則第二基地台執行步驟 329 以更新第二金鑰，再執行步驟 331 以儲存更新後之第二金鑰。最後執行步驟 333，結束金鑰更新之流程。若步驟 327 之判斷結果為是，則直接進入步驟 333 以結束金鑰更新之流程。

除上述步驟外，第二實施例亦能執行第一實施例之無線網路系統之動作且亦具有第一實施例之無線網路系統所具有之功能。所屬技術領域具有通常知識者可直接瞭解第二實施例如何基於上述第一實施例之無線網路系統以執行此等操作，故不贅述。

本發明之第三實施例為一種電腦程式產品，內儲一種用以進行金鑰更新之程式。此電腦程式產品適用於一無線網路系統，此無線網路系統包含一第一基地台及一第二基地台。第一基地台具有一第一訊號範圍，第二基地台具有一第二訊號範圍，其中第一訊號範圍及第二訊號範圍部分重疊。第一基地台使用一第一金鑰，且第二基地台使用一第二金鑰。該程式被載入第一基地台及第二基地台之之微處理器後，可分別執行複數個程式指令，以使微處理器完成前述第二實施例所述之步驟。此電腦程式產品可以是軟碟、硬碟、光碟、隨身碟、磁帶、可由網路存取之資料庫或熟悉此技術者可輕易思及具有相同功能之儲存媒體。

第 4 圖係描繪一無線網路系統 4 之範例，用以比較本發明與習知技術之效能。此無線網路系統 4 包含 N 個基地台，各該基地台具有一訊號範圍，而訊號範圍之重疊方式如第 4 圖所示。假設行動裝置之移動方式為，由最左邊的基地台登入無線網路系統 4，接著往右移動，依序進出所有的基地台，最後由最右方的基地台登出無線網路系統 4。另外假設每次更新金鑰所需的成本為 M。

若採用習知技術，則行動裝置每次進入或離開一基地台，被進入或被離開的那個基地台皆需要更新其使用的金鑰。則當行動裝置依照前述路徑移動時，無線網路系統 4 更新金鑰之成本為 2*N*M。

若採用本發明之技術，最佳的情況為無線網路系統 4 僅在行動裝置由最左邊的基地台登入無線網路系統 4 及由最右邊的基地台登出無線網路系統 4 時需要更新金鑰，因此更新金鑰的成本為

2*M。最糟的情況則是，無線網路系統 4 中只有一行動裝置，因此不論除了前述之登入及登出外，行動裝置於基地台間移動時，基地台亦需更新金鑰，因此更新金鑰的成本為 2*N*M。

第 5 圖係為習知技術與本發明之效能比較圖，所模擬之環境為具有三個基地台之無線網路系統。於初始時，每個基地台之訊號範圍內各有 50 個行動裝置。根據使用者之行為模擬這 150 個行動裝置登入無線網路系統、離開無線網路系統及於基地台間移動（handover）之情形。第 5 圖中，水平方向軸表示於基地台間移動（handover）之比率，垂直方向軸表示更新金鑰次數。由第 5 圖可知，不論於基地台間之移動比率為何，本發明所需之更新金鑰之次數都比習知技術低。此外，當基地台間移動（handover）之比率越高時，本發明所能降低金鑰交換之次數更加顯著。

綜上所述，本發明所揭露之技術，於行動裝置由一原始基地台之訊號範圍移動至一目標基地台之訊號範圍時，目標基地台會判斷是否需要更新其所使用之金鑰。若行動裝置登入無線網路系統之時間晚於目標基地台之金鑰之更新時間，則目標基地台立即更新金鑰，否則便不更新，藉此可降低無線網路系統更新金鑰之次數。

上述之實施例僅用來例舉本發明之實施態樣，以及闡釋本發明之技術特徵，並非用來限制本發明之保護範疇。任何熟悉此技術者可輕易完成之改變或均等性之安排均屬於本發明所主張之範圍，本發明之權利保護範圍應以申請專利範圍為準。

【圖式簡單說明】

第 1 圖係描繪第一實施例之無線網路系統之示意圖；

第 2 圖係描繪金鑰更新裝置之示意圖；

第 3A 圖係描繪第二實施例之金鑰更新方法之部分流程圖；

第 3B 圖係描繪第二實施例之金鑰更新方法之另一部分流程圖；

第 4 圖係描繪用以比較本發明與習知技術之無線網路系統示意圖；以及

第 5 圖係為習知技術與本發明之效能比較圖。

【主要元件符號說明】

1：無線網路系統

103：第二基地台　　105：第二訊號範圍

107：第一基地台　　109：第二訊號範圍

111：行動裝置　　113：行動裝置

A、B、D、E、F、H：位置

4：無線網路系統

五、中文發明摘要：

一種金鑰更新裝置、方法、其電腦程式產品及包含前述裝置之無線網路系統。此方法適用於一第一基地台，該第一基地台屬於一無線網路系統。該第一基地台具有一第一訊號範圍且使用一第一金鑰。該方法包含下列步驟：判斷一行動裝置由一第二基地台所具有之一第二訊號範圍進入該第一訊號範圍；判斷該行動裝置登入該無線網路之一登入時間晚於該第一金鑰之一更新時間；更新該第一金鑰；以及傳送該第一金鑰予該行動裝置。

六、英文發明摘要：(案件名稱：APPARATUS AND METHOD FOR RENEWING A KEY, COMPUTER PROGRAM PRODUCT THEREOF AND WIRELESS NETWORK SYSTEM COMPRISING THE SAME)

Apparatuses and methods for renewing a key, computer program products thereof, and wireless network system comprising the same are provided. The method is adapted to a first base station. The first base station belongs to a wireless network. The first base station uses a first key and has a first signal range. The method comprises the steps of: determining a mobile device moving from the first signal range to a second signal range of a second base station; determining the login time of the mobile device being later than the renewing time of the first key; renewing the first key; and sending the first key to the mobile device.

十、申請專利範圍：

1. 一種金鑰（key）更新方法，適用於一第一基地台，該第一基地台屬於一無線網路系統，該第一基地台具有一第一訊號範圍且使用一第一金鑰，該金鑰更新方法包含下列步驟：

(a)判斷一行動裝置由一第二基地台所具有之一第二訊號範圍進入該第一訊號範圍，其中該第一訊號範圍與該第二訊號範圍部分重疊，該第二基地台屬於該無線網路系統，且該第二基地台使用一第二金鑰；

(b)判斷該行動裝置登入該無線網路系統之一登入時間晚於該第一金鑰之一更新時間；

(c)因應步驟(b)，更新該第一金鑰；以及

(d)傳送該第一金鑰予該行動裝置。

2. 如請求項 1 所述之金鑰更新方法，更包含下列步驟：

於步驟(a)後，記錄該行動裝置離開該第二訊號範圍且該行動裝置曾取得該第二金鑰。

3. 如請求項 1 所述之金鑰更新方法，更包含下列步驟：

於步驟(a)後，記錄該行動裝置進入該第一訊號範圍。

4. 如請求項 1 所述之金鑰更新方法，更包含下列步驟：

(e)判斷該行動裝置離開該第一訊號範圍；以及

(f)記錄該行動裝置離開該第一訊號範圍且該行動裝置曾取得該第一金鑰。

5. 如請求項 4 所述之金鑰更新方法，更包含下列步驟：

(g)判斷該行動裝置係由該第一基地台登出該無線網路系統；

(h)於該步驟(g)後，判斷於該行動裝置離開該第一訊號範圍後，該第一基地台未曾更新該第一金鑰；以及

(i)因應步驟(h)，更新該第一金鑰。

6. 如請求項5所述之金鑰更新方法，更包含下列步驟：

(j)於該步驟(g)後，判斷於該行動裝置離開該第二訊號範圍後，該第二基地台未曾更新該第二金鑰；以及

(k)因應步驟(j)，更新該第二金鑰。

7. 如請求項4所述之金鑰更新方法，更包含下列步驟：

(g)判斷該行動裝置係由該第一基地台登出該無線網路系統；

(h)於該步驟(g)後，判斷於該行動裝置離開該第二訊號範圍後，該第二基地台未曾更新該第二金鑰；以及

(i)因應該步驟(h)，更新該第二金鑰。

8. 一種金鑰更新裝置，適用於一第一基地台，該第一基地台具有一第一訊號範圍，該第一基地台屬於一無線網路系統，該金鑰更新裝置包含：

一儲存模組，用以儲存該第一基地台使用之一第一金鑰；

一處理模組，用以判斷一行動裝置由一第二基地台之一第二訊號範圍進入該第一訊號範圍，用以判斷該行動裝置登入該無線網路系統之一登入時間晚於該第一金鑰之一更新時間，以及用以因應該判斷結果，更新該第一金鑰，其中該第一訊號範圍與該第二訊號範圍部分重疊，該第二基地台屬於該無線網路系統，且該第二基地台使用一第二金鑰；以及

一傳送模組，用以傳送該第一金鑰予該行動裝置。

9. 如請求項 8 所述之金鑰更新裝置，其中該儲存模組更用以記錄該行動裝置進入該第一訊號範圍。

10. 如請求項 8 所述之金鑰更新裝置，其中該處理模組更用以判斷當該行動裝置離開該第一訊號範圍，以及該儲存模組更用以記錄該行動裝置離開該第一訊號範圍，且該行動裝置曾取得該第一金鑰。

11. 如請求項 10 所述之金鑰更新裝置，其中該處理模組更用以判斷該行動裝置係由該第一基地台登出該無線網路系統，再用以判斷於該行動裝置離開該第一訊號範圍後，該第一基地台未曾更新該第一金鑰，以及用以更新該第一金鑰。

12. 一種電腦程式產品，內儲一種用以進行金鑰更新之程式，該電腦程式產品適用於一第一基地台，該第一基地台屬於一無線網路系統，該第一基地台使用一第一金鑰，該程式被載入該第一基地台之一微處理器後執行：

程式指令 A，使該微處理器判斷一行動裝置由一第二基地台之一第二訊號範圍進入該第一訊號範圍，其中該第一訊號範圍與該第二訊號範圍部分重疊，該第二基地台屬於該無線網路系統，且該第二基地台使用一第二金鑰；

程式指令 B，使該微處理器判斷該行動裝置登入該無線網路系統之一登入時間晚於該第一金鑰之一更新時間；

程式指令 C，使該微處理器於執行該程式指令 B 後，更新該第一金鑰；以及

程式指令 D，使該微處理器傳送該第一金鑰予該行動裝置。

13. 如請求項 12 所述之電腦程式產品，其中該程式更執行：

程式指令 E，使該微處理器於執行於程式指令 A 後，記錄該行動裝置離開該第二訊號範圍且該行動裝置曾取得該第二金鑰。

14. 如請求項 12 所述之電腦程式產品，其中該程式更執行：

程式指令 E，使該微處理器於執行於程式指令 A 後，記錄該行動裝置進入該第一訊號範圍。

15. 如請求項 12 所述之電腦程式產品，其中該程式更執行：

程式指令 F，使該微處理器判斷該行動裝置離開該第一訊號範圍；以及

程式指令 G，使該微處理器記錄該行動裝置離開該第一訊號範圍且該行動裝置曾取得該第一金鑰。

16. 如請求項 15 所述之電腦程式產品，其中該程式更執行：

程式指令 H，使該微處理器判斷該行動裝置係由該第一基地台登出該無線網路系統；

程式指令 I，使該微處理器執行於程式指令 G 後，判斷於該行動裝置離開該第一訊號範圍後，該第一基地台未曾更新該第一金鑰；以及

程式指令 J，使該微處理器於執行程式指令 I 後，更新該第一金鑰。

17. 如請求項 16 所述之電腦程式產品，其中該程式更執行：

程式指令K，使該微處理器於執行於程式指令H後，判斷於該行動裝置離開該第二訊號範圍後，該第二基地台未曾更新該第二金鑰；以及

程式指令L，使該微處理器於執行程式指令K後，更新該第二金鑰。

18. 如請求項15所述之電腦程式產品，其中該程式更執行：

程式指令H，使該微處理器判斷該行動裝置係由該第一基地台登出該無線網路系統；

程式指令I，使該微處理器於執行於程式指令H後，判斷於該行動裝置離開該第二訊號範圍後，該第二基地台未曾更新該第二金鑰；以及

程式指令J，使該微處理器於執行該程式指令I後，更新該第二金鑰。

19. 一種無線網路系統，包含：

一第一基地台，具有一第一訊號範圍且使用一第一金鑰；以及

一第二基地台，具有一第二訊號範圍且使用一第二金鑰，其中該第二訊號範圍與該第一訊號範圍部分重疊；

其中，該第一基地台判斷一行動裝置由該第二訊號範圍進入該第一訊號範圍，該第一基地台判斷該行動裝置登入該無線網路系統之一登入時間晚於該第一金鑰之一更新時間，該第一基地台因應該判斷結果，更新該第一金鑰，且該第一基地台傳送更新後之該第一金鑰予該行動裝置。

20. 如請求項19所述之無線網路系統，其中該第二基地台更用以於該行動裝置離開該第二訊號範圍後，記錄該行動裝置離開該第二訊號範圍且該行動裝置曾取得該第二金鑰。

21. 如請求項19所述之無線網路系統，其中該第一基地台更用以於該行動裝置進入該第一訊號範圍後，記錄該行動裝置進入該第一訊號範圍。

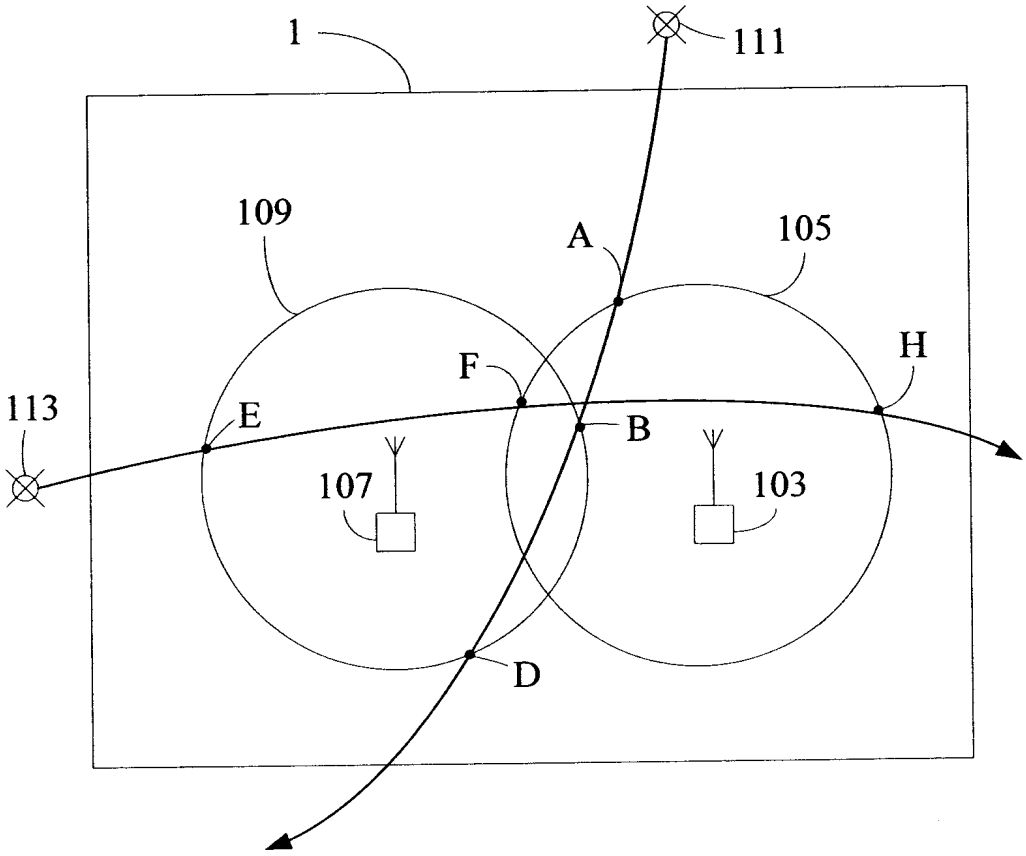
22. 如請求項19所述之無線網路系統，其中該第一基地台更判斷該行動裝置離開該第一訊號範圍，且該第一基地台之後更記錄該行動裝置離開該第一訊號範圍且該行動裝置曾取得該第一金鑰。

23. 如請求項22所述之無線網路系統，其中該第一基地台更判斷該行動裝置係由該第一基地台登出該無線網路系統，該第一基地台之後更判斷於該行動裝置離開該第一訊號範圍後，該第一基地台未曾更新該第一金鑰，以及該第一基地台更新該第一金鑰。

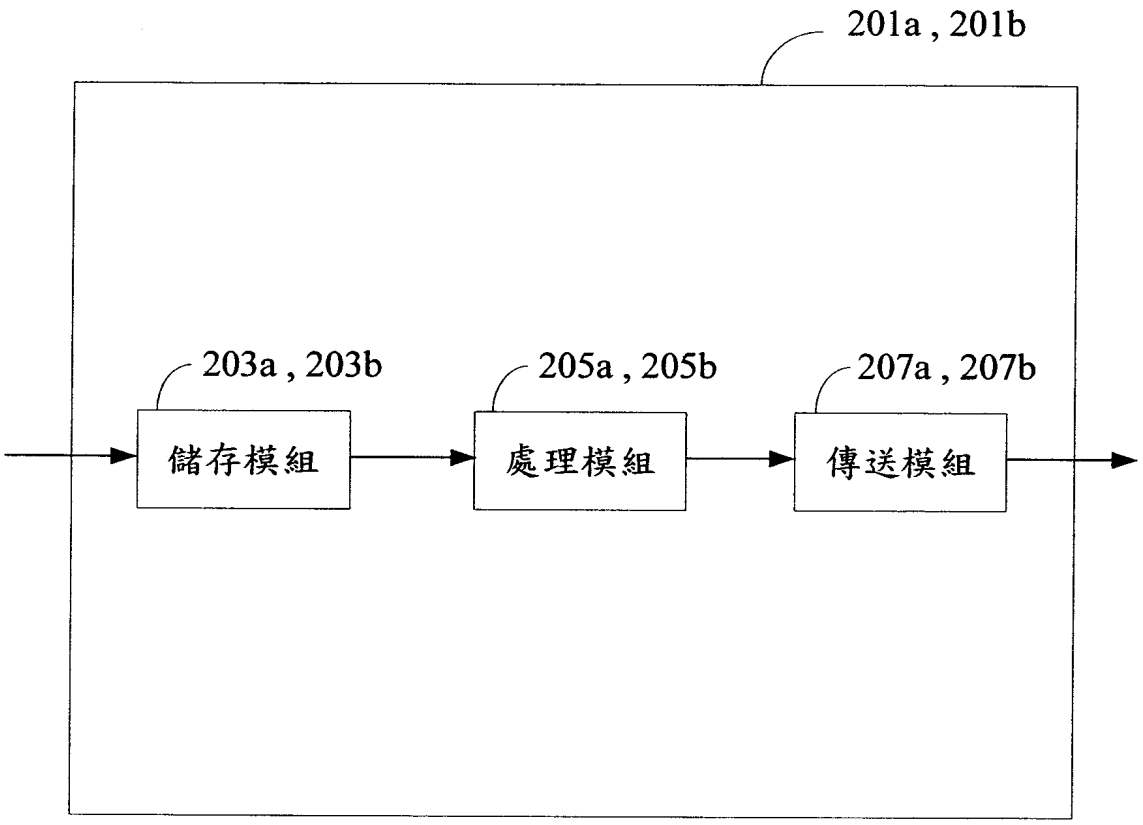
24. 如請求項23所述之無線網路系統，其中該第二基地台更判斷於該行動裝置離開該第二訊號範圍後，該第二基地台未曾更新該第二金鑰，該第二基地台之後更新該第二金鑰。

25. 如請求項22所述之無線網路系統，其中該第一基地台更判斷該行動裝置係由該第一基地台登出該無線網路系統，該第二基地台判斷於該行動裝置離開該第二訊號範圍後，該第二基地台未曾更新該第二金鑰，且該第二基地台更新該第二金鑰。

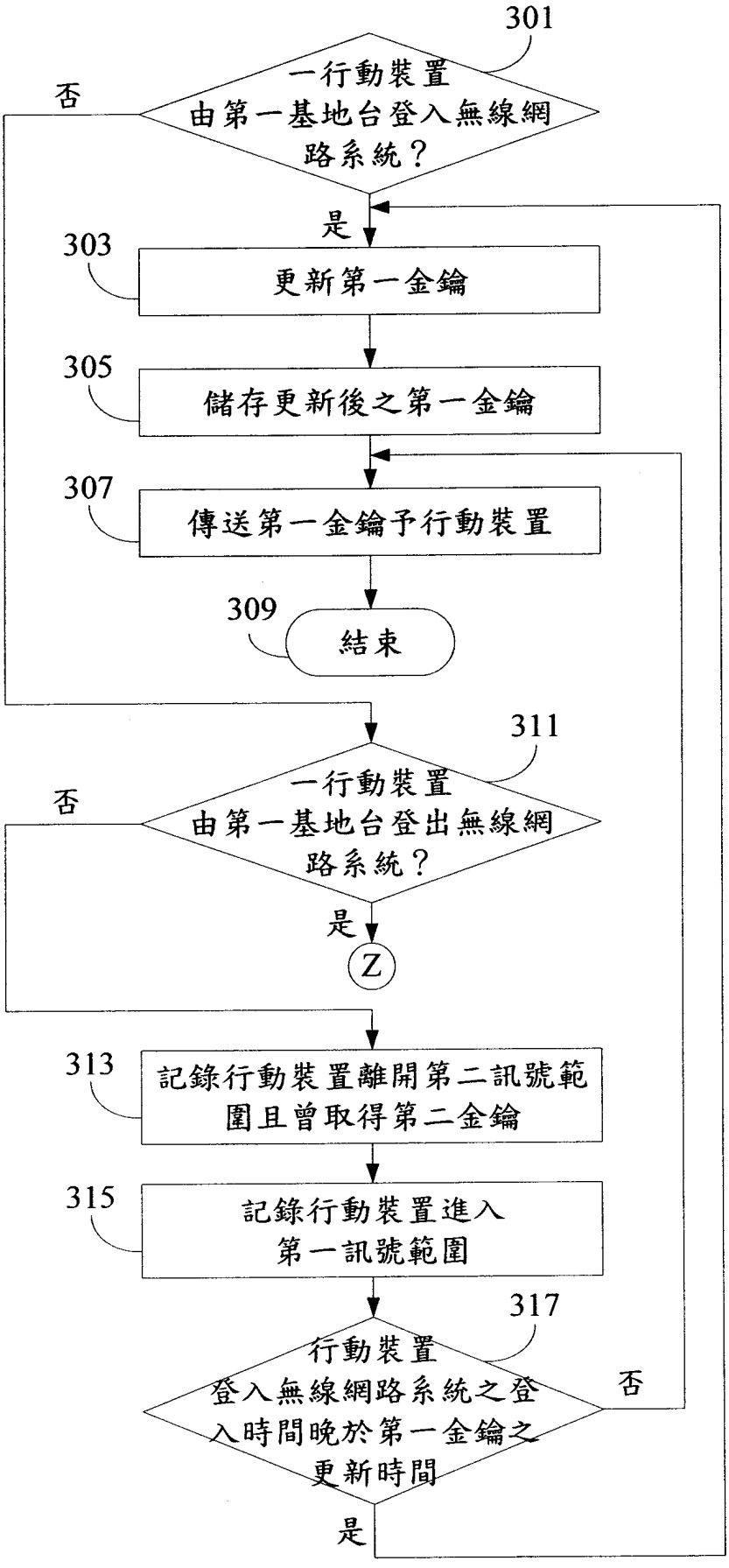
十一、圖式：



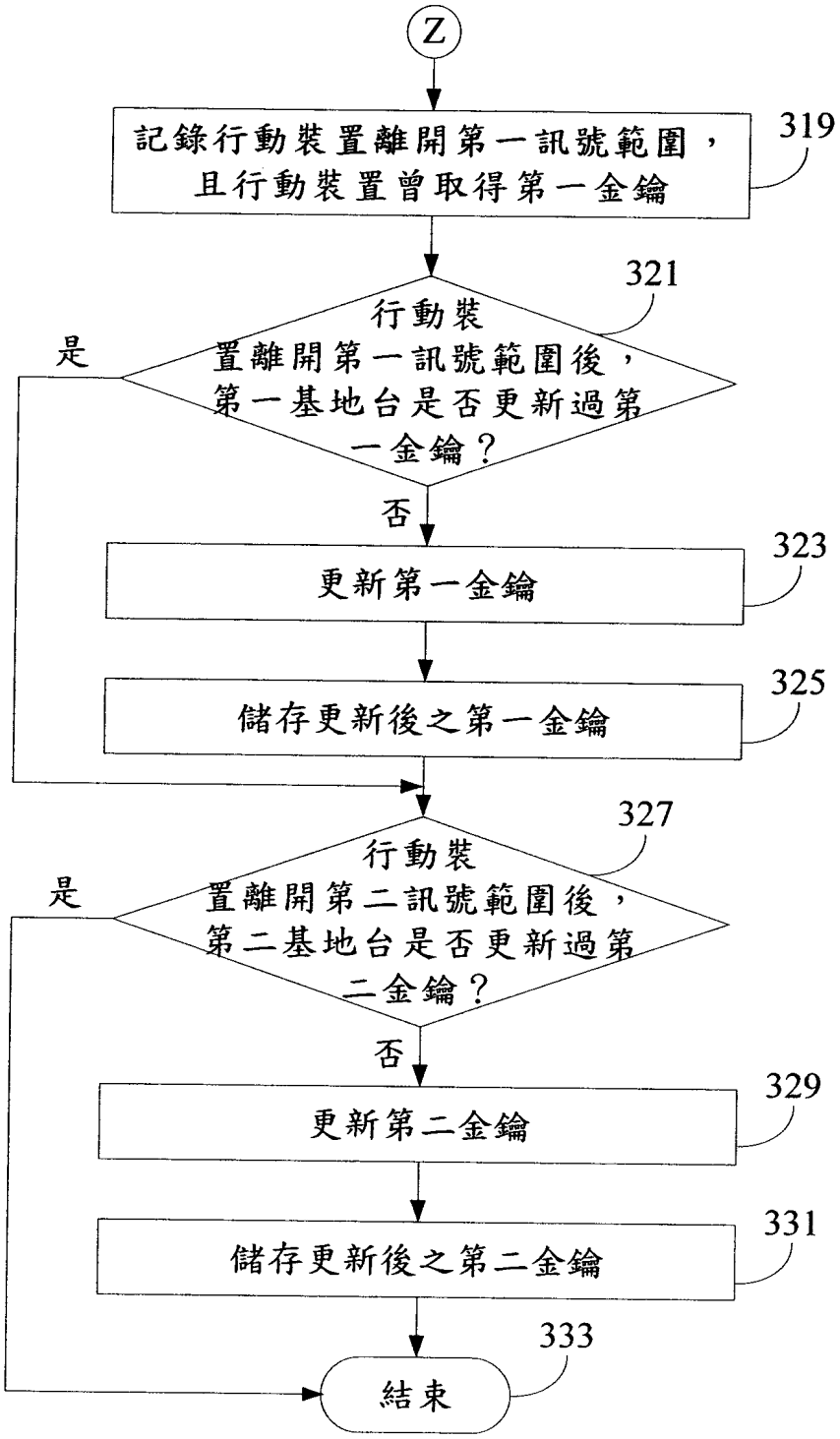
第 1 圖



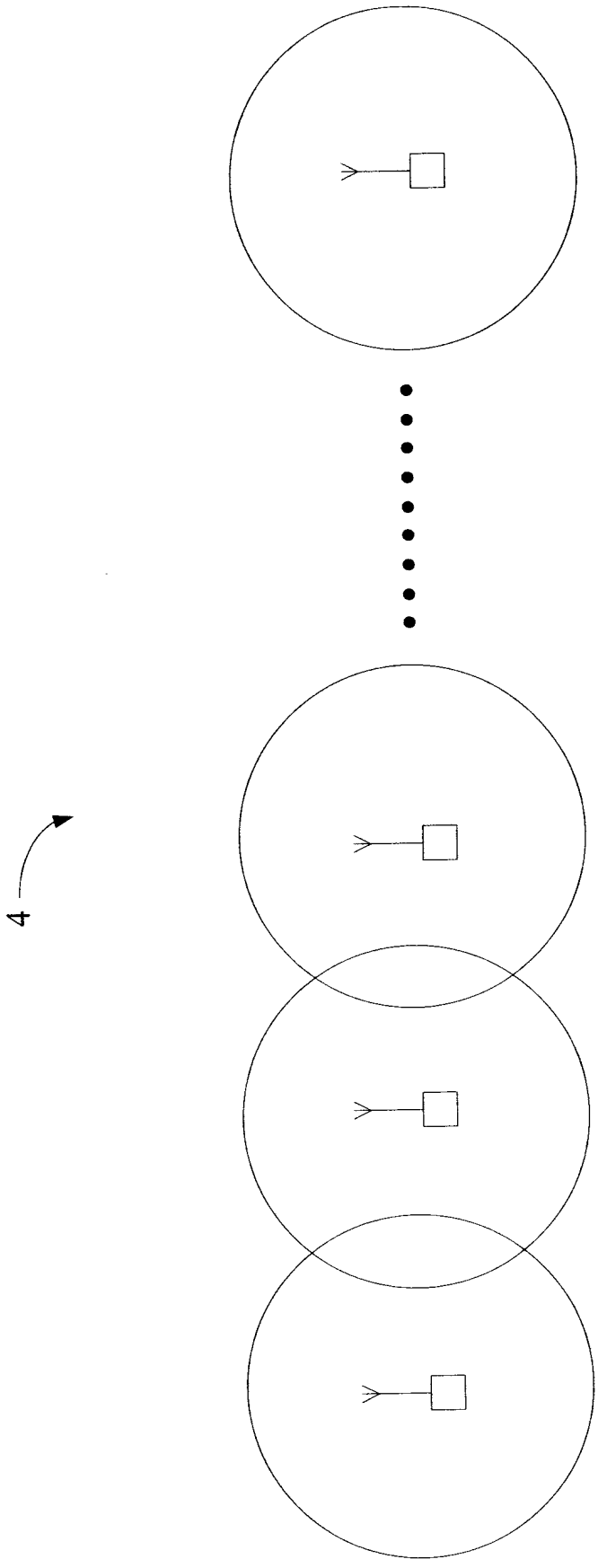
第 2 圖


301
一行動裝置由第一基地台登入無線網路系統？
否
是
303
更新第一金鑰
305
儲存更新後之第一金鑰
307
傳送第一金鑰予行動裝置
309
結束
311
一行動裝置由第一基地台登出無線網路系統？
否
是
Z
313
記錄行動裝置離開第二訊號範圍且曾取得第二金鑰
315
記錄行動裝置進入第一訊號範圍
317
行動裝置登入無線網路系統之登入時間晚於第一金鑰之更新時間
否
是

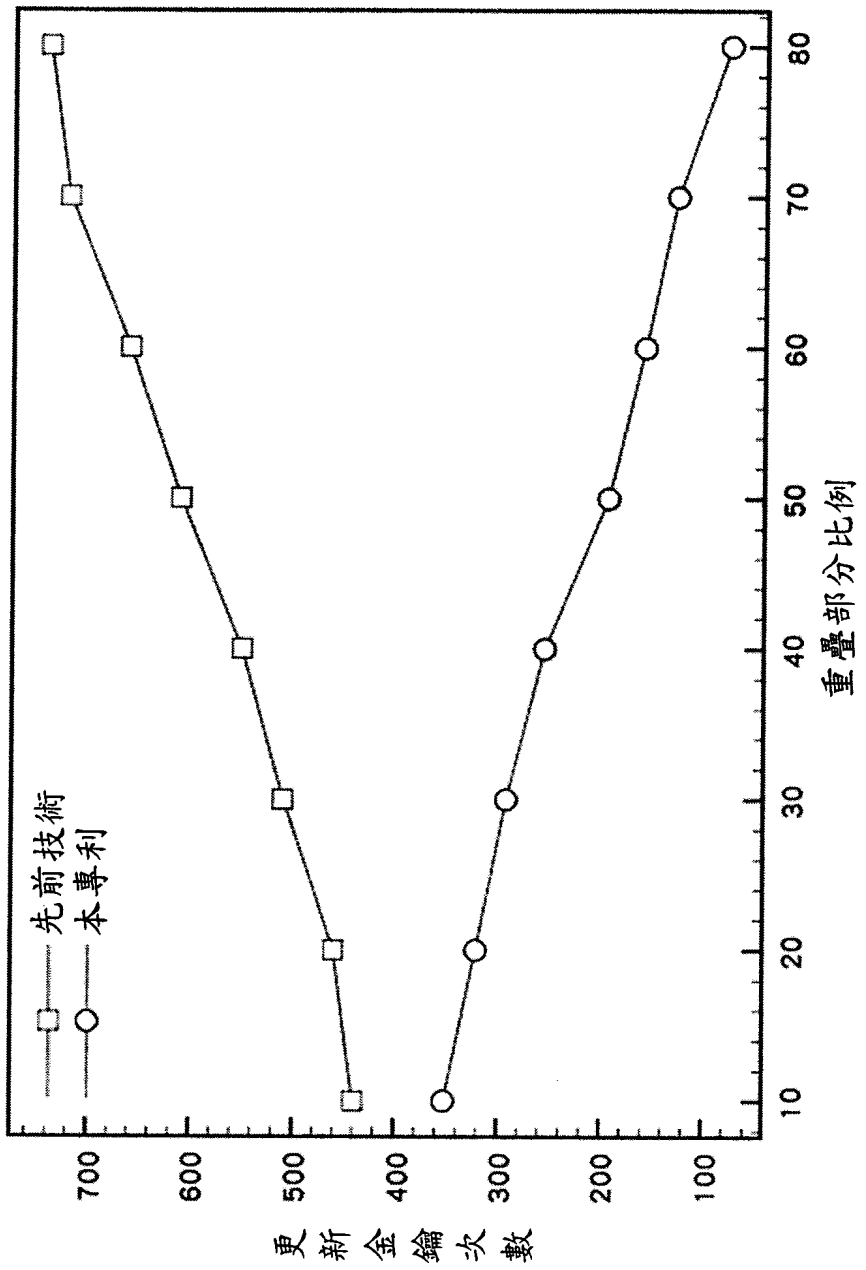
第 3A 圖


Z
記錄行動裝置離開第一訊號範圍，且行動裝置曾取得第一金鑰
319
321
行動裝置離開第一訊號範圍後，第一基地台是否更新過第一金鑰？
是
否
323
更新第一金鑰
325
儲存更新後之第一金鑰
327
行動裝置離開第二訊號範圍後，第二基地台是否更新過第二金鑰？
是
否
329
更新第二金鑰
331
儲存更新後之第二金鑰
333
結束

第 3B 圖



第 4 圖


先前技術
本專利
更新金鑰次數
重疊部分比例
700
600
500
400
300
200
100
10
20
30
40
50
60
70
80

第 5 圖

七、指定代表圖：

(一)本案指定代表圖為：第（1）圖。

(二)本代表圖之元件符號簡單說明:

1：無線網路系統

103：第二基地台

105：第二訊號範圍

107：第一基地台

109：第二訊號範圍

111：行動裝置

113：行動裝置

A、B、D、E、F、H：位置

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：