



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I722497 B

(45)公告日：中華民國 110 (2021) 年 03 月 21 日

(21)申請案號：108125658

(22)申請日：中華民國 105 (2016) 年 03 月 01 日

(51)Int. Cl. : *H04W12/02 (2009.01)**H04W12/06 (2009.01)*

(30)優先權：2015/03/05 美國

62/128,724

2015/07/24 美國

14/808,862

(71)申請人：美商高通公司 (美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：李秀凡 LEE, SOO BUM (KR)；帕拉尼古德 艾納德 PALANIGOUNDER, ANAND

(IN)；伊史考特 愛德利恩愛德華 ESCOTT, ADRIAN EDWARD (GB)；霍恩 蓋

文伯納德 HORN, GAVIN BERNARD (US)

(74)代理人：李世章

(56)參考文獻：

CN 101959183B

CN 101998377B

US 2006/0154646A1

審查人員：鍾瑞元

申請專利範圍項數：20 項 圖式數：7 共 69 頁

(54)名稱

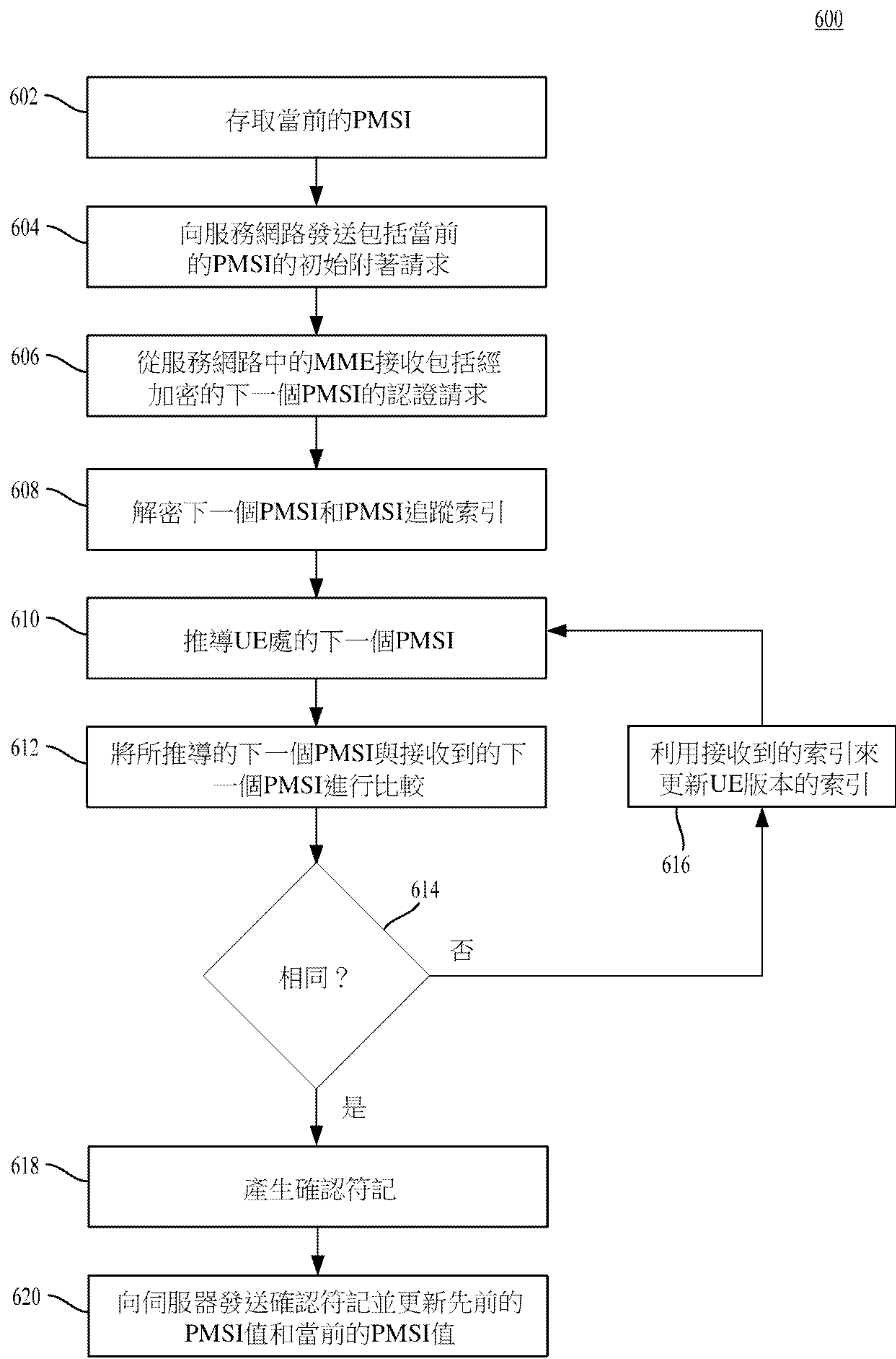
無線網路中的身份私密性

(57)摘要

揭示用於藉由替代地提供私密性行動用戶身份來保護使用者裝備的國際行動用戶身份的系統和方法。在向服務網路的附著嘗試中，UE 提供 PMSI 而不是 IMSI，保護 IMSI 免受洩露。PMSI 是在歸屬網路伺服器與 UE 之間決定的，使得服務網路中的中間節點單元不知曉 PMSI 與 IMSI 之間的關係。在接收到附著請求中的 PMSI 時，伺服器產生要在後續附著請求中使用的下一個 PMSI 並且將該下一個 PMSI 發送給 UE 以進行確認。UE 確認下一個 PMSI 以便在 UE 與伺服器之間進行同步，並且向伺服器發送確認符記。隨後，UE 和伺服器均更新當前和下一個 PMSI 值的本端複本。

Systems and techniques are disclosed to protect a user equipment's international mobile subscriber identity by providing a privacy mobile subscriber identity instead. In an attach attempt to a serving network, the UE provides the PMSI instead of IMSI, protecting the IMSI from exposure. The PMSI is determined between a home network server and the UE so that intermediate node elements in the serving network do not have knowledge of the relationship between the PMSI and the IMSI. Upon receipt of the PMSI in the attach request, the server generates a next PMSI to be used in a subsequent attach request and sends the next PMSI to the UE for confirmation. The UE confirms the next PMSI to synchronize between the UE and server and sends an acknowledgment token to the server. The UE and the server then each update local copies of the current and next PMSI values.

指定代表圖：



符號簡單說明：

600 . . . 示例性方法

602 . . . 步驟

604 . . . 步驟

606 . . . 步驟

608 . . . 步驟

610 . . . 步驟

612 . . . 步驟

614 . . . 決定步驟

616 . . . 步驟

618 . . . 步驟

620 . . . 步驟

圖6A



公告本

I722497

【發明摘要】

【中文發明名稱】無線網路中的身份私密性

【英文發明名稱】IDENTITY PRIVACY IN WIRELESS NETWORKS

【中文】

揭示用於藉由替代地提供私密性行動用戶身份來保護使用者裝備的國際行動用戶身份的系統和方法。在向服務網路的附著嘗試中，UE提供PMSI而不是IMSI，保護IMSI免受洩露。PMSI是在歸屬網路伺服器與UE之間決定的，使得服務網路中的中間節點單元不知曉PMSI與IMSI之間的關係。在接收到附著請求中的PMSI時，伺服器產生要在後續附著請求中使用的下一個PMSI並且將該下一個PMSI發送給UE以進行確認。UE確認下一個PMSI以便在UE與伺服器之間進行同步，並且向伺服器發送確認符記。隨後，UE和伺服器均更新當前和下一個PMSI值的本端複本。

【英文】

Systems and techniques are disclosed to protect a user equipment's international mobile subscriber identity by providing a privacy mobile subscriber identity instead. In an attach attempt to a serving network, the UE provides the PMSI instead of IMSI, protecting the IMSI from exposure. The PMSI is determined between a home network server and the UE so that intermediate node elements in the serving network do not

have knowledge of the relationship between the PMSI and the IMSI. Upon receipt of the PMSI in the attach request, the server generates a next PMSI to be used in a subsequent attach request and sends the next PMSI to the UE for confirmation. The UE confirms the next PMSI to synchronize between the UE and server and sends an acknowledgment token to the server. The UE and the server then each update local copies of the current and next PMSI values.

【指定代表圖】第（ 6A ）圖。

【代表圖之符號簡單說明】

6 0 0 示 例 性 方 法

6 0 2 步 驟

6 0 4 步 驟

6 0 6 步 驟

6 0 8 步 驟

6 1 0 步 驟

6 1 2 步 驟

6 1 4 決 定 步 驟

6 1 6 步 驟

6 1 8 步 驟

6 2 0 步 驟

【特徵化學式】

無

【發明說明書】

【中文發明名稱】無線網路中的身份私密性

【英文發明名稱】IDENTITY PRIVACY IN WIRELESS NETWORKS

【技術領域】

【0001】 本專利申請案請求享有於2015年3月5日提出申請的、名為「Identity Privacy in Wireless Networks」的美國臨時專利申請案第62/128,724號的權益，經由引用將其全部揭示內容併入本文。

【0002】 本案涉及無線通訊系統，並且更具體地說，涉及在無線通訊期間增加用戶身份的私密性。

【先前技術】

【0003】 為了從網路接收服務，未知的使用者裝備（UE）需要向網路進行註冊或以其他方式為網路所知。這是使用網路附著程序來實現的。作為附著程序的一部分，UE發送其國際行動用戶識別（IMSI）號。IMSI是UE在與其進行通訊的（或代表其進行通訊的）所有網路上使用的唯一標識。UE利用附著請求來發送IMSI，該附著請求在行動性管理實體（MME）處接收。

【0004】 在保護IMSI免受竊聽和追蹤的嘗試中，可以在對UE進行初始地認證之後使用臨時行動用戶身份（TMSI）。TMSI對特定區域是本地，因此必須在每個區域中重新分配TMSI。此外，TMSI是在UE提供用於

初始認證的IMSI之後首次分配的（使得TMSI的分配可以與UE的真實身份相關聯）。有時在初始附著請求中提供全球唯一臨時UE身份（GUTI）而不是IMSI。在UE發送GUTI而不是其IMSI的情況下，MME請求來自可能先前已與UE互動的其他網路單元的標識。若UE為其他網路單元所知，則彼等其他網路單元用IMSI來回應。若UE是未知的，則MME要求UE提供其IMSI以進行標識，該IMSI稍後用於具有位置註冊的更新程序。

【0005】 在上面方法中的任何一種方法下，IMSI仍然是易受攻擊的。IMSI被包括在初始附著請求中或必須稍後被提供以便被認證。因此，可以經由空中傳輸量來被動地監測IMSI並使用IMSI來決定用戶身份。附著請求中的IMSI常常是明文，使得IMSI對於監測來說甚至更易受攻擊。甚至在UE不發送IMSI的場景中，MME仍然從其他網路單元獲得實際的IMSI，並且數個不同網路單元可以儲存該實際的IMSI（例如，MME、服務閘道（S-GW）及/或PDN閘道（P-GW））。這使得IMSI是易受攻擊的，並且其依賴於服務網路的可信賴性。

【發明內容】

【0006】 在本案內容的一個態樣中，一種用於由使用者裝備（UE）進行的網路存取的方法包括：利用初始附著訊息，從該UE向網路上的伺服器發送私密性行動用戶身份（PM-SI），以替代國際行動用戶識別（IMSI）來標

識該UE；從該伺服器接收認證請求，該認證請求包括下一個PM-SI，該下一個PM-SI是根據該PM-SI來推導出的不同值；及從該UE向該伺服器發送對該下一個PM-SI的接收確認。

【0007】 在本案內容的另外態樣中，一種使用者裝備包括：記憶體，其被配置為儲存私密性行動用戶身份（PM-SI）；收發機，其被配置為利用初始附著訊息，向網路上的伺服器發送PM-SI，以替代國際行動用戶識別（IMSI）來標識該UE，以及從該伺服器接收認證請求，該認證請求包括下一個PM-SI，該下一個PM-SI是根據該PM-SI來推導出的不同值；及處理器，其被配置為產生接收確認，其中該收發機亦被配置為向該伺服器發送該接收確認。

【0008】 在本案內容的另外態樣中，一種具有記錄在其上的程式碼的電腦可讀取媒體包括：用於使使用者裝備（UE）利用初始附著訊息，向網路上的伺服器發送私密性行動用戶身份（PM-SI），以替代國際行動用戶識別（IMSI）來標識該UE的代碼；用於使該UE從該伺服器接收認證請求的代碼，該認證請求包括下一個PM-SI，該下一個PM-SI是根據該PM-SI來推導出的不同值；及用於使該UE向該伺服器發送對該下一個PM-SI的接收確認的代碼。

【0009】 在本案內容的另外態樣中，一種用於與網路上的伺服器建立網路存取的方法包括：經由中間服務網路中

的一或多個網路單元，經由初始附著訊息來從使用者裝備（UE）接收私密性行動用戶身份（PM-SI），以替代國際行動用戶識別（IM-SI）來標識該UE；由該伺服器基於該PM-SI來決定下一個PM-SI；從該伺服器發送包括該下一個PM-SI的認證請求；及從該UE接收包括對該下一個PM-SI的確認的接收確認。

【0010】 在本案內容的另外態樣中，一種伺服器包括：資料庫，其被配置為儲存使用者裝備（UE）的複數個私密性行動用戶身份（PM-SI）；收發機，其被配置為經由中間服務網路中的一或多個網路單元，經由初始附著訊息來從UE接收私密性行動用戶身份（PM-SI），以替代國際行動用戶識別（IM-SI）來標識該UE；及處理器，其被配置為基於該PM-SI來決定用於該UE的下一個PM-SI，其中該收發機亦被配置為發送包括該下一個PM-SI的認證請求，以及接收包括對該下一個PM-SI的確認的接收確認。

【0011】 在本案內容的另外態樣中，一種具有記錄在其上的程式碼的電腦可讀取媒體包括：用於使伺服器經由中間服務網路中的一或多個網路單元，經由初始附著訊息來從使用者裝備（UE）接收私密性行動用戶身份（PM-SI），以替代國際行動用戶識別（IM-SI）來標識該UE的代碼；用於使該伺服器基於該PM-SI來決定下一個PM-SI的代碼；用於使該伺服器發送包括該下一個PM-SI的認證請求

的代碼；及用於使該伺服器從該UE接收包括對該下一個PMSI的確認的接收確認的代碼。

【圖式簡單說明】

【0012】 圖1圖示根據本案內容的各個態樣的無線通訊網路。

【0013】 圖2是根據本案內容的實施例的示例性UE的方塊圖。

【0014】 圖3是根據本案內容的實施例的示例性伺服器的方塊圖。

【0015】 圖4是根據本案內容的各個態樣，圖示示例性發射器系統的方塊圖。

【0016】 圖5是根據本案內容的各個態樣，圖示在UE、服務網路和歸屬網路之間的、用於支援無線網路中的身份私密性的一些信號傳遞態樣的協定圖。

【0017】 圖6A是根據本案內容的各個態樣，圖示用於UE發起附著程序的示例性方法的流程圖。

【0018】 圖6B是根據本案內容的各個態樣，圖示用於伺服器在附著程序中起作用的示例性方法的流程圖。

【0019】 圖7A是根據本案內容的各個態樣，圖示用於關於UE的PMSI初始化的示例性方法的流程圖。

【0020】 圖7B是根據本案內容的各個態樣，圖示用於關於伺服器的PMSI初始化的示例性方法的流程圖。

【實施方式】

【0021】 下文結合附圖所闡述的詳細描述意欲作為對各種配置的說明，而非意欲表示其中可以以其實踐本文所描述的概念的唯一配置。出於提供對各種概念的透徹理解的目的，詳細描述包括具體的細節。然而，對於本領域技藝人士來說將顯而易見的是，可以在不具有該等具體細節的情況下實踐該等概念。在一些情形中，以方塊圖形式示出公知的結構和元件以便避免混淆該等概念。

【0022】 本文所描述的技術可以用於諸如CDMA、TDMA、FDMA、OFDMA、SC-FDMA和其他網路之類的各種無線通訊網路。術語「網路」和「系統」經常可互換地使用。CDMA網路可以實現諸如通用陸地無線存取（UTRA）、cdma2000等無線技術。UTRA包括寬頻CDMA（WCDMA）以及CDMA的其他變型。

cdma2000涵蓋IS-2000、IS-95和IS-856標準。

TDMA網路可以實現諸如行動通訊全球系統（GSM）之類的無線技術。OFDMA網路可以實現諸如進化的UTRA（E-UTRA）、超行動寬頻（UMB）、IEEE 802.11（Wi-Fi）、IEEE 802.16（WiMAX）、IEEE 802.20、快閃OFDMA等無線技術。UTRA和E-UTRA是通用行動電信系統（UMTS）的一部分。3GPP長期進化（LTE）和進階的LTE（LTE-A）是UMTS的使用E-UTRA的新版本。在來自名為「第三代合作夥伴計畫」（3GPP）的組織的文件中描述了UTRA、E-UTRA、UMTS、LTE、

L T E - A 和 G S M 。在來自名為「第三代合作夥伴計畫 2」（3 G P P 2）的組織的文件中描述了 C D M A 2 0 0 0 和 U M B 。本文所描述的技術可以用於上文提到的無線網路和無線技術以及其他無線網路和無線技術，諸如下一代（例如，第五代（5 G））網路。本案內容的實施例是針對於可以在上文記載的網路及/或有待開發的網路中的任意一或多個網路上使用的任意類型的調制方案。

【0023】 本案內容的實施例介紹了用於藉由替代地提供私密性行動用戶身份（P M S I）來保護使用者裝備的國際行動用戶身份的系統和技術。在一個實施例中，U E 向服務網路發起附著請求。不是提供 I M S I 或該服務網路上的一些單元可以仍然用來存取該 I M S I 的關聯資訊，而是 U E 為 P M S I 提供附著請求。隨後，在整個程序中使用 P M S I，使得在 U E 與伺服器之間不需要 I M S I。在一個實施例中，每個 P M S I（用於每個 U E 以及用於特定 U E 的不同迭代二者）是與眾不同的。這保護 I M S I 免受竊聽和免受服務網路中的任何潛在的惡意單元之害。繼續該實例，服務網路的單元向 U E 的歸屬網路上的伺服器（例如，歸屬用戶伺服器（H S S））傳遞 P M S I 作為認證資訊請求的一部分。H S S 定位到 P M S I 以標識相應的 U E 並且向網路單元提供認證資訊回應。作為該回應的一部分，H S S 亦推導 U E 用於後續附著請求的下一個 P M S I，檢查 P M S I 衝突，並且向服務網路中的網路單元提供下一個 P M S I 和 P M S I 追蹤索引以便傳遞給 U E。

【0024】 可以以加密形式提供下一個PMSI和PMSI追蹤索引。以加密的形式，下一個PMSI和PMSI追蹤索引仍被保護免受服務網路中潛在的惡意網路單元之害和免受竊聽。UE接收所加密的下一個PMSI和PMSI追蹤索引，並且能夠對其進行解密。UE推導出其自身的下一個PMSI副本以確認UE和HSS是同步的。在確認下一個PMSI在UE與HSS之間是同步的之後，UE向伺服器發送確認符記（token）。隨後，UE和伺服器均更新當前和下一個PMSI值的本端複本。HSS不需要為UE儲存PMSI的每次迭代。相反地，HSS可以基於初始PMSI值和期望的PMSI追蹤索引值來得出PMSI的任意迭代。

【0025】 在進一步的實施例中，初始PMSI可以是在UE與HSS之間商定的。在一個實施例中，初始PMSI是在用戶註冊時商定的，使得將初始PMSI供應給UE的SIM卡並且註冊到HSS。在另一個實施例中，UE在用戶註冊時未被供應有PMSI，而是發起與HSS的空中註冊。UE可以產生初始PMSI值，並且在使用HSS的公共金鑰（或者UE與HSS之間的其他共享金鑰）來加密該初始PMSI值之後，向HSS發送所建議的初始PMSI。HSS可以利用相應的私密金鑰來解密來自UE的初始PMSI並且決定該PMSI是否與向HSS註冊的任何其他現有PMSI值相衝突。在確認不存在衝突後，HSS可以向UE確認初始PMSI並且儲存該初始PMSI以便在UE稍後發起其第一附著請求時使用。

【0026】 圖1圖示根據本案內容的各個態樣的無線通訊網路100。無線通訊網路100可以包括多個UE 102以及多個基地台104。僅出於簡化說明和解釋起見，圖1中已圖示單個UE 102和單個基地台104。基地台104可以包括進化型節點B（eNodeB）。基地台亦可以被稱為基地台收發台或存取點。

【0027】 如所示出的，基地台104與UE 102通訊。UE 102可以經由上行鏈路和下行鏈路與基地台104通訊。下行鏈路（或前向鏈路）代表從基地台104到UE 102的通訊鏈路。上行鏈路（反向鏈路）代表從UE 102到基地台104的鏈路。

【0028】 UE 102可以散佈於整個無線網路100，並且每個UE 102可以是固定的或移動的。UE 102亦可以被稱為終端、行動站、用戶單元等。UE 102可以是蜂巢式電話、智慧型電話、個人數位助理、無線數據機、膝上型電腦、平板電腦等。無線通訊網路100是應用本案內容的各個態樣的網路的一個例子。

【0029】 圖1中亦圖示行動性管理實體（MME）106。MME 106可以負責與用戶（例如，UE 102）和通信期管理有關的控制平面功能。例如，MME 106可以提供行動性通信期管理以及對交遞到其他網路、漫遊和用戶認證的支援。MME 106可以輔助在UE 102的初始附著期間的S-GW的選擇、非存取層（NAS）訊號傳遞、NAS訊號傳遞安全、P-GW選擇、包括專用承載建立的承載管理

功能、訊號傳遞傳輸量的合法監聽和其他功能，再次僅舉幾個例子。MME 106和基地台104可以在同一個服務網路108（例如，進化的封包核心（EPC）的一部分）中。將認識到，出於簡化對本案內容的態樣的論述起見，服務網路108包括圖1中未圖示的許多其他網路單元。

【0030】 MME 106與歸屬網路114中的伺服器112通訊。在一個實施例中，伺服器112是歸屬用戶伺服器（HSS），除了其他事項之外，其維護歸屬位置暫存器（HLR），HLR負責對保存使用者訂閱資訊的一或多個資料庫進行儲存和更新。除了其他事項之外，歸屬網路114中的伺服器112具有UE 102的IMSI（使用者標識/定址）的副本。伺服器112亦可以保存使用者簡檔資訊，該使用者簡檔資訊標識服務訂閱狀態及/或服務品質（QoS）資訊（例如，最大允許的位元速率、允許的傳輸量類別等）。伺服器112亦可以包括認證功能，諸如管理根據使用者身份金鑰來產生的安全資訊和該安全資訊向HLR（和其他網路實體）的供應。利用安全資訊，可以執行網路-UE認證。出於簡化說明和解釋的目的，圖1中圖示一個伺服器112。歸屬網路114可以包括多個HSS。例如，HSS的數量可以取決於行動用戶的數量、設備容量和網路組織。MME 106可以經由網路110來與伺服器112通訊，將認識到，這可以是各種類型的直接或間接連接。

【0031】 如下文參照後續的附圖（該附圖包括圖示在 UE、服務網路和歸屬網路（以及相關聯的伺服器）之間的、用於支援無線網路中的身份私密性的一些信號傳遞態樣的協定圖）將更詳細描述的，UE 102 可以將 IMSI 排除在外，使用私密性行動用戶身份（PM SI）來與服務網路 108 和歸屬網路 114 通訊。PM SI 可以是與 UE 102 特定地相關聯的唯一號碼，並由 UE 102 和伺服器 112 保存。在本案內容的實施例中，PM SI 可以包括在 UE 102 和伺服器 112 二者處商定並保持的初始 PM SI。用於 UE 102 的 PM SI 的特定值可以使用一次，使得在後續每次 UE 102 發起附著請求時提供新的 PM SI 值作為該請求的一部分。UE 102 和伺服器 112 可以僅儲存商定的初始 PM SI 以及索引。因此，可以基於初始 PM SI 和用於描述應當執行多少次推導迭代以在 UE 102 和伺服器 112 二者處得出特定 PM SI 的特定索引值的共享知識，來後續地推導出任何 PM SI 值（例如，使得 UE 102 和伺服器 112 關於用於給定通信期的特定 PM SI 保持一致）。

【0032】 在一個例子中，UE 102 可以將其 PM SI 而不是 IMSI 作為其初始附著請求的一部分發送給基地台 104。隨後，基地台 104 將具有 UE 的 PM SI 的附著請求轉發給 MME 106。MME 106 將 PM SI 包括在去往歸屬網路 114 的伺服器 112 的認證資訊請求中。伺服器 112 能夠基於在來自 MME 106 的初始附著請求 / 認證資訊請求中提供的 PM SI 來標識 UE 102，使得不必向服務網路 108

提供IMSI。從伺服器112回到UE 102的通訊亦同樣基於/包括PM SI而不是IMSI。通訊路徑中的所有該等階段使用PM SI而不是IMSI減少了UE 102與基地台104之間的空中竊聽的風險，並且消除了從服務網路108中的任何網路單元對UE 102的IMSI的可獲得性，這是由於將儲存PM SI而不是IMSI。

【0033】圖2是根據本案內容的實施例的示例性UE 102的方塊圖。UE 102可以具有上文所描述的許多種配置中的任何一種。UE 102可以包括處理器202、記憶體204、PM SI模組208、收發機210和天線216。該等單元可以例如經由一或多個匯流排來彼此直接或間接地通訊。

【0034】處理器202可以包括被配置為執行本文中參照上文針對圖1介紹的和下文更詳細論述的UE 102所描述的操作的中央處理單元（CPU）、數位訊號處理器（DSP）、應用特定積體電路（ASIC）、控制器、現場可程式化閘陣列（FPGA）設備、另一種硬體設備、韌體設備，或其任意組合。處理器202亦可以實現為計算設備的組合，例如DSP和微處理器的組合、複數個微處理器、一或多個微處理器連同DSP核心，或任何其他此種結構。

【0035】記憶體204可以包括快取記憶體（例如，處理器202的快取記憶體）、隨機存取記憶體（RAM）、磁阻RAM（MRAM）、唯讀記憶體（ROM）、可程式化唯讀記憶體（PROM）、可抹除可程式化唯讀記憶體

(E P R O M)、電子可抹除可程式化唯讀記憶體 (E E P R O M)、快閃記憶體、固態記憶體設備、硬碟、其他形式的揮發性和非揮發性記憶體，或不同類型的記憶體的組合。在一個實施例中，記憶體 204 包括非暫時性電腦可讀取媒體。記憶體 204 可以儲存指令 206。指令 206 可以包括以下指令：當該等指令由處理器 202 執行時，使處理器 202 執行本文中結合本案內容的實施例參照 U E 102 所描述的操作。指令 206 亦可以被稱為代碼。術語「指令」和「代碼」應被廣義地理解為包括任何類型的電腦可讀取語句。例如，術語「指令」和「代碼」可以代表一或多個程式、常式、子常式、函數、程序等。「指令」和「代碼」可以包括單個電腦可讀取語句或許多個電腦可讀取語句。

【0036】 P M S I 模組 208 可以用於本案內容的各個態樣。例如，P M S I 模組 208 可以涉及初始供應於特定 U E 102 的 P M S I。在一個實施例中，P M S I 可以與用於 U E 102 的 I M S I 同時被供應給 U E 102。例如，在一些情形中，在向 H S S（例如，圖 1 中的伺服器 112）進行用戶註冊的期間供應 P M S I 連同 I M S I。可以在製造時在 U E 102 上的 S I M 卡中發生此種供應。在另一個實施例中，可以在 U E 102 與伺服器 112 之間商定 P M S I 之前供應 I M S I。例如，在已經供應了用於 U E 102 的 I M S I 之後，U E 102 和伺服器 112 可以經由空中來商定第一（初始）P M S I。當經由空中商定了 P M S I 時，U E 102 可以產生建議的初

始 P M S I（如下文關於圖 7 A 將更詳細論述的）並且利用伺服器 1 1 2 所提供的公共金鑰來加密該建議的初始 P M S I。以此方式，可以保護由 U E 1 0 2 發送的該建議的初始 P M S I 免受竊聽和免受服務網路 1 0 8 中潛在受損害的網路單元之害。伺服器 1 1 2 保存相應的私密金鑰並且能夠解密該建議的初始 P M S I。伺服器 1 1 2 可以對照一或多個資料庫檢查該建議的初始 P M S I，以驗證不存在與由歸屬網路 1 1 4 中的伺服器 1 1 2 或其他單元保存的、任何其他 U E 的 P M S I 的衝突。

【 0 0 3 7 】 P M S I 模組 2 0 8 可以額外地涉及到 P M S I 確認中。如前述，特定的 P M S I（基於初始 P M S I）可以僅用於預定數量的附著請求（例如，一個、兩個、三個或更多個），使得為後續附著請求提供不同的 P M S I 值。回應於來自 U E 1 0 2 的附著請求，伺服器 1 1 2 可以產生「下一個 P M S I」（將在後續通信期中使用的下一個 P M S I 值），並且將其作為回應於初始附著請求的認證請求的一部分來與 U E 1 0 2 共享該下一個 P M S I。U E 1 0 2 的 P M S I 模組 2 0 8 可以基於所儲存的初始 P M S I 和遞增的索引（如下文進一步所論述的）來計算其自身的下一個 P M S I 值，並且將本端計算出的下一個 P M S I 與從伺服器 1 1 2 接收的下一個 P M S I 進行比較。若存在匹配，則 P M S I 模組 2 0 8 可以使 U E 1 0 2 產生用於向伺服器 1 1 2 確認該下一個 P M S I 的回應。若不存在匹配，則 P M S I 模組 2 0 8 可以利

用從具有下一個PMSI的伺服器112接收的索引來更新其本端索引，使得在重新計算之後，該等值匹配。

【0038】 收發機210可以包括數據機子系統212和射頻（RF）單元214。收發機210被配置為與其他設備（例如，基地台104）雙向地通訊。數據機子系統212可以被配置為根據調制和編碼方案（MCS）（例如，低密度校驗（LDPC）編碼方案、turbo編碼方案、迴旋編碼方案等）對來自PMSI模組208的資料進行調制及/或編碼。RF單元214可以被配置為對來自數據機子系統212（在向外傳輸上）的經調制/經編碼的資料或源自於諸如基地台104之類的另一個源的傳輸的經調制/經編碼的資料進行處理（例如，執行類比數位轉換或數位類比轉換等）。儘管示出為與收發機210集成在一起，但是數據機子系統212和RF單元214可以是單獨的設備，該等單獨的設備在UE 102處耦合在一起以使得UE 102能夠與其他設備通訊。

【0039】 RF單元214可以將經調制及/或經處理的資料（例如，資料封包（或者，更一般地，可包含一或多個資料封包或其他資訊（包括PMSI值）的資料訊息））提供給天線216以便傳輸到一或多個其他設備。這可以包括例如根據本案內容的實施例的向基地台104的對資料訊息的傳輸。天線216亦可以接收從基地台104發送的資料訊息並且提供所接收的資料訊息以便在收發機210處進行處理及/或解調。儘管圖2將天線216示出為單個天線，

但是天線 216 可以包括具有相似或不同設計的多個天線以便支援多個傳輸鏈路。

【0040】圖 3 是圖示根據本案內容的實施例的示例性伺服器 112 的方塊圖。伺服器 112 可以包括處理器 302、記憶體 304、PMSI 模組 308、資料庫 310 和收發機 312。該等單元可以例如經由一或多個匯流排來彼此直接或間接地通訊。如上文參照圖 1 所提到的，伺服器 112 可以是提供歸屬位置暫存器和認證功能（僅舉兩個例子）的 HSS。

【0041】處理器 302 可以包括被配置為執行本文中參照上文在圖 1 中介紹的伺服器 112 所描述的操作的 CPU、DSP、ASIC、控制器、FPGA 設備、另一種硬體設備、韌體設備，或其任意組合。處理器 302 亦可以實現為計算設備的組合，例如 DSP 和微處理器的組合、複數個微處理器、一或多個微處理器連同 DSP 核心，或任何其他此種結構。

【0042】記憶體 304 可以包括快取記憶體（例如，處理器 302 的快取記憶體）、RAM、MRAM、ROM、PROM、EPROM、EEPROM、快閃記憶體、固態記憶體設備、一或多個硬碟、其他形式的揮發性和非揮發性記憶體，或不同類型的記憶體的組合。在一個實施例中，記憶體 304 包括非暫時性電腦可讀取媒體。記憶體 304 可以儲存指令 306。指令 306 可以包括以下的指令：當該等指令由處理器 302 執行時，使處理器 302 執行本文中結合本案內容的

實施例參照伺服器 112 所描述的操作。指令 306 亦可以被稱為代碼，其可以被廣義地解釋為包括任何類型的電腦可讀取語句，如上文參照圖 2 所論述的。

【0043】 PMSI 模組 308 可以用於本案內容的各個態樣。例如，PMSI 模組 308 可以涉及到初始供應用於特定 UE 102 的 PMSI。在一個實施例中，PMSI 可以與用於 UE 102 的 IMSI 同時（例如在用戶註冊期間）被供應和儲存在資料庫 310 中。在另一個實施例中，可以在伺服器 112 與 UE 102 之間商定 PMSI 之前供應 IMSI。例如，在已經供應了用於 UE 102 的 IMSI 之後，伺服器 112 可以經由空中與 UE 102 商定第一（初始）PMSI。當經由空中商定了時，伺服器 112 可以從 UE 102 接收由 UE 102 產生的建議的初始 PMSI（如下文關於圖 7B 將更詳細論述的）。該建議的初始 PMSI 可能已利用由伺服器 112 向 UE 102 提供的公共金鑰來加密。因此，伺服器 112 可以使用相應的私密金鑰來解密該建議的初始 PMSI。以此方式，可以保護 PMSI 免受竊聽和免受服務網路 108 中潛在受損害的網路單元之害。伺服器 112 可以對照資料庫 310 中的 PMSI 值檢查該建議的初始 PMSI，以驗證不存在與由歸屬網路 114 中的伺服器 112 或其他單元保存的、任何其他 UE 的 PMSI 的衝突。

【0044】 PMSI 模組 308 可以額外地涉及到與 UE 102 的初始附著程序中。伺服器 112 可以接收具有來自 UE 的初始附著請求來的 PMSI，並且對照資料庫 310 中所儲存

的 P M S I 值檢查該 P M S I。回應於來自 U E 1 0 2 的附著請求，伺服器 1 1 2 可以產生下一個 P M S I，並且將其作為回應於初始附著請求的認證請求的一部分來向 U E 1 0 2 發送該下一個 P M S I。回應於從 U E 1 0 2 接收到用於確認下一個 P M S I 的回應，P M S I 模組 3 0 8 更新在資料庫 3 1 0 中所儲存的 P M S I 值。例如，當前 P M S I 值變為先前的 P M S I 值並且下一個 P M S I 值變為用於後續互動（例如，來自 U E 1 0 2 的後續附著請求）的當前 P M S I 值。

【0045】 出於論述的目的，本文提及了四種 P M S I 值：（1）初始 P M S I，其是 U E 1 0 2 和伺服器 1 1 2 用於推導後續 P M S I 值的初始商定的 P M S I 值；（2）當前 P M S I，其是在當前附著請求程序中使用的 P M S I 值（例如，U E 1 0 2 第一次發送初始附著請求時，當前 P M S I 可以等於初始 P M S I，而在其他實施例中可以對 P M S I 進行迭代一次或多次，使得即使在初始附著請求期間亦保持初始 P M S I 較安全）；（3）在先的或先前的 P M S I，其是在當前 P M S I 之前的 P M S I（例如，在先前附著請求中使用的 P M S I 及 / 或用於得出當前 P M S I 的 P M S I）；及（4）下一個 P M S I，其是跟在當前 P M S I 後面的 P M S I（例如，針對商定應當將怎樣的 P M S I 用於 U E 1 0 2 發起的、與任何給定服務網路 1 0 8 的下一個附著程序，U E 1 0 2 和伺服器 1 1 2 二者推導出的 P M S I）。

【0046】 資料庫 3 1 0 可以包括由伺服器 1 1 2 維護的一或多個資料庫，例如上文參照圖 1 所提到的 H L R。資料庫

310 可以追蹤諸如使用者標識和定址之類的用戶資訊（包括例如 IMSI、PM SI（包括初始 PM SI、當前 PM SI、先前的 PM SI 及 / 或下一個 PM SI）、PM SI 追蹤索引和所有用戶或用戶子集的行動電話號碼）、簡檔資訊（例如，服務訂閱狀態）、以及與每個用戶相關聯的安全資訊（例如，安全金鑰）。

【0047】收發機 312 使得伺服器 112 能夠進行通訊以向外部源發送資料和從外部源接收資料，該等外部源諸如歸屬網路 114 或服務網路 108 中的其他網路單元。收發機 312 可以實現無線及 / 或有線通訊。將認識到，收發機 312 可以包括例如以太網路連接、WiFi 連接，或其他類型的數據機及 / 或 RF 子系統。

【0048】圖 4 是根據本案內容的某些態樣，圖示 MIMO 系統 400 中的示例性發射器系統 410（例如，基地台 104）和接收器系統 450（例如，UE 102）的方塊圖。在發射器系統 410 處，從資料來源 412 向發射（TX）資料處理器 414 提供多個資料串流的傳輸量資料。根據本案內容的態樣，該傳輸量資料可以包括各種各樣的傳輸量，其包括來自一或多個 MME 實體的認證請求。

【0049】在下行鏈路傳輸中，例如，在各自的發射天線上發送每個資料串流。TX 資料處理器 414 基於為每個資料串流選定的特定編碼方案來對該資料串流的傳輸量資料進行格式化、編碼和交錯以提供經編碼的資料。

【0050】 可以使用 OFDM 技術將每個資料串流的經編碼的資料與引導頻資料多工在一起。引導頻資料（例如，引導頻序列）通常是已知的資料模式，其以已知方式被處理並且可以在接收器系統處用於估計通道回應或其他通道參數。可以將引導頻資料格式化成引導頻符號。可以由處理器 430 執行的指令來決定引導頻符號的數量和引導頻符號在 OFDM 符號內的放置。

【0051】 隨後，基於為每個資料串流選定的特定調制方案（例如，BPSK、QSPK、M-PSK 或 M-QAM）來對該資料串流的多工的引導頻和編碼資料進行調制（亦即，符號映射）以提供調制符號。可以由處理器 430 執行的指令來決定每個資料串流的資料速率、編碼和調制。亦可以由處理器 430 執行的指令來決定引導頻符號的數量和引導頻符號在每個訊框中的放置，例如如上文參照圖 2 或圖 3 所描述的。發射器系統 410 亦包括記憶體 432，例如如上文參照圖 2 或圖 3 所描述的。

【0052】 隨後將所有資料串流的調制符號提供給 TX MIMO 處理器 420，TX MIMO 處理器 420 可以進一步處理調制符號（例如，針對 OFDM）。隨後，TX MIMO 處理器 420 將 N_T 個調制符號串流提供給 N_T 個發射器（TMR）422_a 至 422_t。在一些實施例中，TX MIMO 處理器 420 向資料串流的符號以及向從其發送符號的天線應用波束成形權重。發射器系統 410 包括具有僅一個天線或具有多個天線的實施例。

【0053】 每個發射器422接收並處理各自的符號串流以提供一或多個類比信號，並且進一步調節（例如，放大、濾波和升頻轉換）類比信號以提供適合於在MIMO通道上傳輸的調制信號。隨後，從 N_T 個天線424_a至424_t分別發送來自發射器422_a至422_t的 N_T 個調制符號。本文所描述的技術亦應用於具有僅一個發射天線的系統。使用一個天線的傳輸比多天線場景要簡單。例如，在單天線場景中可能不需要TX MIMO處理器420。

【0054】 在接收器系統450處，由 N_R 個天線452_a至452_r接收所發送的調制信號，並且將從每個天線452接收的信號提供給各自的接收器（RCVR）454_a至454_r。每個接收器454調節（例如，濾波、放大和降頻轉換）各自的接收信號，對經調節的信號進行數位化以提供取樣，並且進一步處理取樣以提供相應的「接收到的」符號串流。本文所描述的技術亦應用於具有僅一個天線452的接收器系統450的實施例。

【0055】 隨後，RX資料處理器460基於特定的接收器處理技術從接收器454_a至454_r接收並處理 N_R 個接收符號串流，以提供 N_T 個經偵測的符號串流。隨後，RX資料處理器460根據需要對每個經偵測的符號串流進行解調、解交錯和解碼，以恢復資料串流的傳輸量資料。根據本案內容的態樣，所恢復的傳輸量可以包括例如來自MME的認證資訊請求中的資訊。由RX資料處理器460

進行的處理可以與在發射器系統410處由TX MIMO處理器420和TX資料處理器414執行的處理互補。

【0056】 由RX資料處理器460所提供的資訊允許處理器470產生諸如通道狀態資訊(CSI)和其他資訊之類的報告以提供給TX資料處理器438。處理器470制定(formulate)包括CSI及/或引導頻請求的反向鏈路訊息以發送給發射器系統。

【0057】 處理器470可以實現成例如上文關於圖2或圖3中描述的處理器所描述的。除了反向鏈路訊息之外，接收器系統450可以發送其他各種類型的資訊，包括附著請求、確認符記和用於建立通訊通信期的其他資訊以及在通訊通信期的資料。訊息可以由TX資料處理器438進行處理、由TX MIMO處理器480進行調制、由發射器454_a至454_r進行調節，並且被發送回發射器系統410。如所示出的，TX資料處理器438亦可以從資料來源436接收多個資料串流的傳輸量資料。

【0058】 在發射器系統410處，來自接收器系統450的調制信號由天線424進行接收、由接收器422進行調節、由解調器440進行解調，並且由RX資料處理器442進行處理，以提取由接收器系統450所發送的反向鏈路訊息。因此，可以在發射器系統410與接收器系統450之間發送和接收資料。將認識到，發射器系統410亦可以用於將其從接收器系統450接收的資訊發送給其服務網路內的其他網路單元以及從服務網路中的一或多個其他網路單元

接收資訊。圖4中示出的實施例僅是示例性的，本案內容的實施例適用於未在圖4中示出的其他發射器/接收器系統。

【0059】 圖5是根據本案內容的各個態樣，圖示在UE、服務網路和歸屬網路（以及伺服器）之間的、用於支援無線網路中的身份私密性的一些信號傳遞態樣的協定圖。為了簡化論述，在描述圖5的協定圖中的動作時將引用圖1中示出的單元（例如，UE 102、基地台104（其作為eNB）、MME 106以及伺服器112（其作為HSS））。進一步出於簡化起見，論述將聚焦於協定流的對本案內容的實施例的態樣進行描述的彼等態樣而不是附著程序的所有態樣（例如，論述將聚焦於除了具有一些重疊的3GPP標準（例如在TS 23.401 5.3.2.1中找到的，或其他附著程序）以外的態樣或不同於具有一些重疊的3GPP標準的態樣）。

【0060】 在動作502中，UE 102存取在UE 102中所儲存的當前PM SI。在UE 102第一次嘗試附著到服務網路108的情況下，當前PM SI可以對應於初始PM SI（例如，其中PM SI是與UE 102的IM SI同時被供應的，或者其中PM SI是在稍後但在附著請求之前商定的）。在在在的附著程序已發生的實施例中或者由於在伺服器112處的PM SI衝突而成為必要的實施例中，儲存在UE 102中的當前PM SI是在在在的附著程序期間UE與伺服器112之間商定的下一個PM SI。UE 102可以儲存一或多

個 P M S I 值，包括初始 P M S I、當前 P M S I、先前的 P M S I 及 / 或下一個 P M S I。在一些情形中，當前 P M S I 儲存成與先前的 P M S I 值不同的值。

【0061】 在一些實施例中，U E 102 根據先前的 P M S I 和 P M S I 追蹤索引來推導當前 P M S I。例如，對於初始 P M S I，P M S I 追蹤索引可以初始化為 0，並且每次 U E 102 和伺服器 112 成功地完成附著程序時，可以在 U E 102 和伺服器 112 處將 P M S I 追蹤索引遞增固定值（例如，1）。因此，U E 102 和伺服器 112 中的每一個可以儲存 [初始 P M S I，P M S I 追蹤索引]，其可以用於得出當前在使用中的 P M S I 的任何迭代。每一個亦可以儲存 [當前 P M S I，P M S I 追蹤索引] 並且依賴於 P M S I 追蹤索引來決定是否需要替代地引用初始 P M S I（例如，當索引值在 U E 102 與伺服器 112 之間不匹配時）。

【0062】 在動作 504，U E 102 例如藉由向基地台 104 發送初始附著請求，來向服務網路 108 發送初始附著請求，該初始附著請求隨後前進至 M M E 106。初始附著請求包括當前 P M S I 而不是 I M S I（或服務網路 108 內的一或多個單元可以用於與 U E 102 的 I M S I 進行關聯的任何其他值）。

【0063】 在 M M E 106 在動作 504 期間接收到初始附著請求之後，在動作 506，M M E 106 取得初始附著請求中的資訊並且向伺服器 112 發送認證資訊請求。該認證資訊

請求可以包括當前 PMSI 和序號，該序號代表 UE 102 正在存取的服務網路 108。

【0064】 在動作 508，在伺服器 112 在動作 506 期間已接收到認證資訊請求之後，伺服器 112 檢查認證資訊請求中所包括的 PMSI 並且（除了別的操作之外）對照一或多個資料庫檢查 PMSI。作為動作 508 的一部分，伺服器 112 對 PMSI 進行解密（當 PMSI 已被加密時）。例如，伺服器 112 可以使用與用於對 PMSI 進行加密的公共金鑰相關聯的私密金鑰來對 PMSI 進行解密。伺服器 112 將 PMSI 與例如在上文圖 3 中描述的資料庫 310 中所儲存的值進行比較。當伺服器 112 發現 PMSI 值之間的匹配時，伺服器 112 亦可以檢查與從 UE 102 接收的當前 PMSI 相對應的 IMSI。

【0065】 當存在 PMSI 值的匹配時，作為動作 508 的一部分，伺服器 112（例如，PMSI 模組 308）可以推導下一個 PMSI 以便包括在去往 MME 106 的認證回應中。在一個實施例中，如以下推導下一個 PMSI。將 PMSI 追蹤索引遞增一固定量（例如，1）並且將其串聯到資料庫 310 中所儲存的當前 PMSI 值（如在來自 MME 106 的認證資訊請求中所標識的）。該值作為輸入連同 K_{PMSI} 值被包括到另一個推導函數中。 K_{PMSI} 是 PMSI 產生金鑰。例如， K_{PMSI} 可以是藉由使用金鑰推導函數（KDF）來建立的，該 KDF 具有原始金鑰 K（例如，EPS 主金鑰）和 PMSI 推導上下文 CTX 作為輸入（例如， $K_{PMSI} = KDF(K, CTX)$ ）。

CTX))。CTX可以是上下文，例如，諸如「PM SI產生」之類的字串—藉由在金鑰產生中使用上下文，可以使用相同的金鑰K來產生不同的金鑰，諸如藉由併入不同的上下文來得到有差異的金鑰產生結果。

【0066】與索引串聯的 $K_{PM SI}$ 值和PM SI在函數中一起被散列化（例如，（結果 = $HMAC(K_{PM SI}, PM SI | \text{索引})$ ），其中|是串聯運算元）。可以對函數的結果進行截斷，使得將HMAC函數的輸出（帶金鑰的散列訊息認證碼）限制到固定數量的數位（例如，9-10個數位）。隨後可以將該截斷的結果與行動網路碼（MNC）和行動服務國家碼（MCC）串聯並且所得值變為下一個PM SI。作為截斷的結果，在一個實施例中該值可以是15個數位長，但是將認識到，在不脫離本案內容的範圍的情況下，其他長度（更長和更短）是可能的。在一個實施例中，可以如下描述整個運算：

下一個PM SI = $MCC | MNC | \text{截斷}(HMAC(K_{PM SI}, PM SI | \text{索引}))$. （公式1）

【0067】一般而言，伺服器112可以儲存PM SI（例如，初始及/或當前PM SI）與PM SI追蹤索引。PM SI追蹤索引使得伺服器112能夠藉由對初始PM SI重複地散列化x次來根據初始PM SI計算當前PM SI，其中x等於PM SI追蹤索引值。PM SI追蹤索引對於計帳以及對於衝突避免亦是有用的。例如，伺服器112可以對照其他已知的PM SI值來檢查所產生的下一個PM SI，以驗證不存在

與任何其他 UE 的 PMSI 的衝突。在存在衝突的情況下，伺服器 112 可以將索引遞增（例如，遞增 1）並且利用新的 PMSI-串聯-索引值來重複公式（1）。

【0068】 在動作 510，伺服器 112 取得所產生的資訊並且將其併入到要發送給 MME 106 的認證資訊回應中。可以為了認證資訊回應中增加的安全性而對下一個 PMSI 進行加密，例如，使得 MME 106 不能夠區分在 UE 102 與伺服器 112 之間的下一個 PMSI。例如，可以利用根據 K_{PMSI} 和亂數（RAND）推導出的匿名金鑰（例如，匿名金鑰 = 函數（ K_{PMSI} ，RAND））來對下一個 PMSI 進行加密。

【0069】 匿名金鑰是藉由將 K_{PMSI} 和亂數 RAND 放置到金鑰推導函數中作為輸入而推導出的。金鑰推導函數可以是符合 3GPP 標準（或未來等同/相似的標準）的任何推導函數，例如 f5*。在一個實施例中，金鑰推導函數可以是 HMAC 函數。因此，在一個實施例中，匿名金鑰可以是由 $HMAC(K_{PMSI}, RAND)$ 推導出的。在替代的實施例中，匿名金鑰可以是金鑰加密金鑰（KEK），其中啟用了初始服務網路 108 認證。

【0070】 作為動作 510 的一部分，伺服器 112 可以向 MME 106 發送認證資訊回應。認證資訊回應可以包括（除了其他內容以外）認證向量和加密形式的下一個 PMSI/PMSI 追蹤索引（如由以上描述了其推導的匿名函數所加密的）。在一個實施例中，認證向量自身可以包括

認證符記、期望的回應、亂數和本端主金鑰 K_{ASME} 。因此，除了傳統上認證向量可以包括的彼等以外，本案內容的實施例亦包括用於與 UE 102 同步的下一個 PMSI 和 PMSI 追蹤索引。MME 106 可以儲存認證向量，但是在一些實施例中，其不儲存經加密的 PMSI/PMSI 追蹤索引。

【0071】 在動作 512，MME 106 藉由向 UE 102 發送認證請求來參與與 UE 102 的相互認證。認證請求帶有從動作 510 的認證資訊回應獲得的資訊。例如，MME 106 可以保持期望的回應作為認證的一部分，並且傳遞認證符記、亂數、eUTRAN 金鑰集識別符（eKSI）以及經加密的下一個 PMSI 和 PMSI 追蹤索引。

【0072】 在動作 514，UE 102（除了與 MME 106 的傳統相互認證程序以外）確認下一個 PMSI 並且產生用於返回給伺服器 112 的確認符記。關於這一點，UE 102 從在動作 512 中接收的認證請求中解密出經加密的下一個 PMSI 和 PMSI 追蹤索引值。UE 102 能夠解密下一個 PMSI 和 PMSI 追蹤索引值，因為 UE 102 具有伺服器 112（而不是 MME 106）亦具有的共享秘密金鑰 CTX（PMSI 推導金鑰）。

【0073】 UE 102 自身推導出下一個 PMSI，以便與由伺服器 112 所產生的下一個 PMSI 進行比較以確認其是否是同步的。UE 102 可以藉由利用下一個 PMSI 追蹤索引對當前 PMSI 進行散列化來推導下一個 PMSI。或者，

UE 102 可以藉由對初始 PMSI 重複地散列化 x 次來推導下一個 PMSI，其中 x 等於 PMSI 追蹤索引值（如 UE 102 本端地保存的或如從伺服器 112 解密出的）。隨後 UE 102 將本端推導出的下一個 PMSI 與從伺服器 112 接收的下一個 PMSI 進行比較。若值匹配，則 UE 102 可以繼續產生確認符記。

【0074】 若這兩個下一個 PMSI 值不匹配（例如，當 UE 102 使用其自身版本的 PMSI 追蹤索引時），則 UE 102 和伺服器 112 不是同步的。這可能例如在來自 UE 102 的訊息或去往 UE 102 的訊息在途中被丟棄的情形中發生。在該場景中，UE 102 可以更新其 PMSI 追蹤索引以對應於從伺服器 112 接收和解密的 PMSI 追蹤索引。隨後 UE 102 可以重新推導下一個 PMSI 並將其與從伺服器 112 接收和解密的下一個 PMSI 再次進行比較。

【0075】 在下一個 PMSI 被確認的情況下（該下一個 PMSI 將用作針對後續附著程序的當前 PMSI 值），UE 102 可以繼續產生確認符記。可以藉由串聯經加密的序號（用於同步）和 MAC-A 值來產生確認權杖符記。加密態樣包括對在 UE 102 與伺服器 112 之間共享的序號進行加密。加密可以是經由另一個匿名金鑰來執行的，在一個實施例中，該另一個匿名金鑰不同於上文在動作 510 所描述的匿名金鑰（例如，這裡匿名金鑰是使用符合 3GPP 標準或其他標準的不同函數來推導的）。例如，用於加密序號

的匿名金鑰自身可以是由採用上文所描述的 K_{PMSE} 和亂數作為輸入的各種金鑰推導函數中的任何一種來產生的。

【0076】串聯到經加密的序號的 $MAC-A$ 值是根據訊息認證函數（例如， $f1^*$ ）來產生的，訊息認證函數採用另一個匿名金鑰（例如，不同於上文所描述的其他匿名金鑰中的任何一種）、與亂數串聯的序號和認證管理欄位（ AMF ）值作為輸入。用作訊息認證函數中的輸入的匿名金鑰可以是藉由採用 K_{PMSE} 和亂數作為輸入的另一個金鑰推導函數來產生的。出於簡化論述起見，描述了該等函數和特定的輸入。將認識到，在不脫離本案內容的範圍的情況下，可以使用其他的函數和對該等函數的其他輸入。

【0077】在動作 516， $UE\ 102$ 將在動作 514 產生的確認符記發送回給 $MME\ 106$ 和伺服器 112 作為 $PMSI$ 確認訊息。 $PMSI$ 確認訊息可以包括上文關於動作 514 所產生和描述的認證符記，以及亂數（例如，上文在金鑰推導函數中使用的相同亂數）。在一個實施例中，可以利用附著程序的其他態樣（例如，加密的選項回應訊息）從 $UE\ 102$ 向 $MME\ 106$ 捎帶（piggyback） $PMSI$ 確認訊息，這裡沒有詳細描述。在 $MME\ 106$ 處，可以利用發送給伺服器 112 的另一個訊息（例如，更新位置請求）從 $MME\ 106$ 向伺服器 112 捎帶 $PMSI$ 確認訊息。

【0078】在動作 518，在接收到確認符記時，伺服器 112 用當前 $PMSI$ 值來更新先前的 $PMSI$ ，並用下一個

PMSI 值（其已經由 UE 102 進行確認，並因此是同步的）來更新當前 PMSI。這是有用的，使得在附著程序中使用的 PMSI 值可以仍然在建立的通訊期在伺服器 112、服務網路 108 和 UE 102 之間使用，例如在向其他 MME 的交遞期間，使得 UE 102 的位置可以向伺服器 112 適當地更新而無需披露 UE 102 的 IMSI。儘管根據本案內容，任何對 IMSI 的使用由對 PMSI 的使用來替換，但該附著程序隨後可以繼續包括傳統上執行的其他態樣。

【0079】 在 UE 102 的成功認證之後，例如參照圖 5 所描述的，依據一些管轄區域的法律，可能要求伺服器 112 向諸如圖 1 中示出的服務網路 108 之類的請求服務網路披露 UE 102 的 IMSI。根據本案內容的態樣，在該等情況下伺服器 112 可以仍然供應 PMSI 來替代 IMSI 以防範一或多個惡意網路單元（例如惡意的 MME 106）的可能性。

【0080】 此種請求可能呈現為如下（儘管在圖 5 中未圖示）。MME 106 可以向伺服器 112 發送對 UE 102 的 IMSI 請求。根據本案內容的實施例，由於 MME 106 在附著程序（或交遞）期間沒有接收到 UE 102 的 IMSI 而是接收到 PMSI，因此 MME 106 包括所接收的與 UE 102 相關聯的 PMSI 連同 K_{IMSI} 加密金鑰。 K_{IMSI} 加密金鑰可以產生為來自函數（例如，具有 K_{ASME} （存取安全管理實體）和 IMSI 取回金鑰作為輸入的 HMAC 函數）的結果。 K_{ASME} 是 MME 106 基本金鑰，其對於 MME 106 和伺服器 112 皆是已知的。

【0081】 回應於IMSI請求，伺服器112提供IMSI回應。在一個實施例中，在MME 106不具有用來得出IMSI的其他能力的情況下，伺服器112發送PM SI。這是可能的，例如，由於伺服器112仍然保持著UE 102的PM SI與IMSI（其是IMSI請求的主題）之間的關聯，並且因此出於所有意圖，PM SI提供所請求的驗證，這是因為伺服器112將能夠如使用IMSI一樣使用PM SI來存取相同的資訊。在另一個實施例中，伺服器112利用PM SI以及加密版本的IMSI來進行回應。例如，伺服器112可以取得PM SI和IMSI並且使用 K_{IMSI} 來對其進行加密。因此，可以僅由有效地擁有 K_{ASME} 的MME 106來正確地解密IMSI。

【0082】 現在轉到圖6A，根據本案內容的各個態樣，流程圖圖示用於UE使用PM SI來發起附著程序的示例性方法600。可以在與服務網路108（例如，僅示出服務網路108的兩個網路單元，基地台104和MME 106）相通訊的UE 102中實現方法600。出於簡化論述起見，將參照特定的UE 102來描述方法600，但是將認識到的，本文所描述的態樣可以適用於複數個UE 102。應當理解，可以在方法600的步驟之前、期間和之後提供額外的步驟，並且對於方法600的其他實施例來說，可以替換或消除所描述的步驟中的一些步驟。

【0083】 在步驟602，UE 102存取當前PM SI，該當前PM SI將用於在步驟604處的初始附著請求。如上文參

照圖 5 所論述的，若對於 UE 102 而言是第一次附著嘗試，則當前 PMSI 可以是在 UE 102 處（例如，在記憶體 204 中）所儲存的初始 PMSI。在在在的附著程序已發生的其他實施例中，當前 PMSI 是在在在的附著程序期間在伺服器 112 與 UE 102 之間確認的下一個 PMSI。

【0084】 在步驟 604，一旦取得當前 PMSI，UE 102 就向當前服務網路（例如，如圖 1 中所示出的 108）發送初始附著請求。初始附著請求包括所取得的當前 PMSI（而不是 IMSI 或可以用於重構 UE 102 的 IMSI 的其他值）以及其他資訊。初始附著請求可以由基地台 104 接收，基地台 104 將該請求轉發給 MME 106。在 MME 106 接收到初始附著請求之後，MME 106 取得初始附著請求中的資訊並且向伺服器 112 發送具有 PMSI 而不是 IMSI 的認證資訊請求。

【0085】 在步驟 606，UE 102 從服務網路 108 中的 MME 106（例如，經由基地台 104）接收認證請求（例如如上文在圖 5 的動作 512 處所描述的）。認證請求可以包括來自伺服器 112 的經加密的下一個 PMSI 和 PMSI 追蹤索引，MME 106 可能無法存取該經加密的下一個 PMSI 和 PMSI 追蹤索引，因為其不具有適當的金鑰來進行解密。

【0086】 在步驟 608，UE 102 對從 MME 106 接收的作為認證請求的一部分的下一個 PMSI 和 PMSI 追蹤索引值進行解密。UE 102 能夠對下一個 PMSI 和 PMSI 追蹤

索引值進行解密，因為UE 102具有伺服器112在產生用於加密該等值的匿名金鑰時所使用的共享秘密金鑰，如上文參照圖5的動作508和514所描述的。

【0087】 在步驟610，UE 102自身推導下一個PM SI值（亦即，無需依賴於在步驟608處接收的下一個PM SI和PM SI追蹤索引）。在一個實施例中，UE 102基於在UE 102處（例如，在記憶體204中）所儲存的先前的PM SI值和PM SI追蹤索引值來推導下一個PM SI值。在另一個實施例中，UE 102基於儲存在UE 102中的初始PM SI值以及PM SI追蹤索引的當前值來推導下一個PM SI值（例如，對PM SI值進行散列化若干次，該次數等於PM SI追蹤索引的當前值）。

【0088】 在步驟612，UE 102（例如，處理器202與PM SI模組208合作）將本端推導出的下一個PM SI值與所接收和解密的下一個PM SI值進行比較。

【0089】 在決定步驟614，若本端推導出的下一個PM SI值與所接收和解密的下一個PM SI值不匹配，則方法600行進到步驟616，其中在步驟616，UE 102將其本端版本的PM SI追蹤索引更新為等於從伺服器112接收和解密的PM SI追蹤索引的值。隨後方法600從步驟616行進回到步驟610，在步驟610該程序如上文所描述的繼續進行。

【0090】 返回到決定步驟614，若本端推導出的下一個PMSI值與所接收和解密的下一個PMSI值確實匹配，則方法600行進到步驟618。

【0091】 在步驟618，UE 102（例如，處理器202與PMSI模組208合作）產生要向伺服器112發送の確認符記，例如如上文參照圖5的動作514所描述的。

【0092】 在步驟620，UE 102例如經由服務網路108的一或多個網路單元向伺服器112發送所產生的確認符記。UE 102亦例如藉由以下方式來更新其本端PMSI值：更新先前的PMSI以反映當前PMSI值（在當前附著程序中使用的PMSI），以及更新當前PMSI以反映同步的下一個PMSI值。將認識到，UE 102和服務網路108可以繼續建立通訊通信期。

【0093】 圖6B是根據本案內容的各個態樣，圖示用於伺服器在附著程序中使用PMSI的示例性方法630的流程圖。可以在與服務網路108（例如，僅示出服務網路108的一個網路單元例子，MME 106）相通訊的伺服器112中實現方法630。出於簡化論述起見，將參照伺服器112來描述方法630，但是將認識到的，本文所描述的態樣可以適用於複數個伺服器112。應當理解，可以在方法630的步驟之前、期間和之後提供額外的步驟，並且對於方法630的其他實施例來說可以替換或消除所描述的步驟中的一些步驟。

【0094】 在步驟632，伺服器112從服務網路108（例如，MME 106）接收認證資訊請求，該認證資訊請求包括由UE 102提供給MME 106的當前PM SI而不是UE 102的IM SI。如上文參照動作506所描述的，MME 106基於該MME 106從UE 102接收的初始附著請求來發送認證資訊請求。

【0095】 在步驟634，伺服器112（例如，處理器302與PM SI模組308和資料庫310合作）對照已在伺服器112處保存（或可由伺服器112從別處存取）的PM SI值檢查所接收的PM SI，以標識與所接收的PM SI相對應的特定UE 102，例如如上文關於圖5的動作508所描述的。

【0096】 在步驟636，在發現匹配之後，伺服器112對位於資料庫310中（或可由伺服器112從別處存取）的、與所接收的PM SI相關聯的PM SI追蹤索引進行遞增。PM SI追蹤索引由伺服器112保存並保持與UE的PM SI記錄相關聯。PM SI追蹤索引使得伺服器112能夠基於在UE 102與伺服器112之間商定的初始PM SI來計算UE 102的PM SI的任何迭代，如上文所描述的。此種用於得出PM SI值的任何迭代的能力亦使得伺服器112能夠實現各種計帳和計費目的。伺服器112亦使用PM SI追蹤索引來解決以下情形：其中在由伺服器112推導的可能的下一個PM SI值與已在伺服器112處保存的用於另一個UE 102的另一個PM SI值之間發生衝突。在一個實施例中，舉例而言，可以將PM SI追蹤索引遞增值1。

【0097】 在步驟638，伺服器112（例如，處理器302與PMSI模組308合作）推導下一個PMSI。伺服器112可以基於在步驟632處在認證資訊請求中接收的當前PMSI以及來自步驟636的遞增的PMSI追蹤索引來推導下一個PMSI，例如如上文參照圖5中的動作508所描述的。類似地，伺服器可以基於初始PMSI和PMSI追蹤索引值來推導下一個PMSI。

【0098】 在決定步驟640，伺服器112對照其他已知的PMSI值檢查在步驟638處推導的下一個PMSI，以驗證不存在與任何其他UE的PMSI的衝突。若存在衝突，則方法630行進回到步驟636，其中在步驟636再次遞增PMSI追蹤索引，並且隨後在步驟638利用新的PMSI追蹤索引值來推導下一個PMSI。

【0099】 返回到決定步驟640，若不存在衝突，則方法630行進到步驟642。在步驟642，伺服器112對下一個PMSI和遞增的PMSI追蹤值進行加密，例如如上文參照圖5中的動作508所描述的。如圖5中所論述的，可以將經加密的下一個PMSI和PMSI追蹤索引值與認證資訊回應連同認證向量包括在一起。

【0100】 在步驟644，伺服器112向MME 106發送包括經加密的下一個PMSI和PMSI追蹤索引值的認證資訊回應。隨後，MME 106可以參與與UE 102的相互認證。作為該相互認證的一部分，MME 106可以發送經加密的

下一個 P M S I 和 P M S I 追蹤索引值而無需在此處 M M E 1 0 6 已解密該資訊。

【0101】 在 U E 1 0 2 確認下一個 P M S I 值之後，例如根據圖 6 A 的步驟 6 0 8 - 6 1 6 中的一或多個步驟，方法 6 0 0 行進到步驟 6 4 6。在步驟 6 4 6，一旦 U E 1 0 2 確認了下一個 P M S I 值或者以其他方式完成了同步（例如，藉由發送新建議的下一個 P M S I 值、請求新的下一個 P M S I 值，或調整其本端 P M S I 追蹤索引以反映所接收和解密的 P M S I 追蹤索引的值），伺服器 1 1 2 經由 M M E 1 0 6 從 U E 1 0 2 接收認證符記。作為回應，伺服器 1 1 2 隨後更新其 P M S I 資訊（例如，伺服器 1 1 2 更新先前的 P M S I 以反映當前 P M S I 值（在當前附著程序中使用的 P M S I）並且更新當前 P M S I 以反映同步的下一個 P M S I 值）。將認識到，U E 1 0 2 和服務網路 1 0 8 可以繼續建立通訊通信期。

【0102】 現在轉到圖 7 A，根據本案內容的各個態樣，流程圖圖示用於關於 U E 的 P M S I 初始化的示例性方法 7 0 0。可以在與基地台 1 0 4 和 M M E 1 0 6 相通訊的 U E 1 0 2 中實現方法 7 0 0。出於簡化論述起見，將參照單個 U E 1 0 2 來描述方法 7 0 0，但是將認識到的，本文所描述的態樣可以適用於複數個 U E 1 0 2。應當理解，可以在方法 7 0 0 的步驟之前、期間和之後提供額外的步驟，並且對於方法 7 0 0 的其他實施例來說可以替換或消除所描述的步驟中的一些步驟。

【0103】 在步驟702，UE 102開始初始化程序。這可以發生在供應（provisioning）UE 102的時候（例如，利用根據本案內容的態樣的IMSI和PM SI值對UE 102的SIM卡進行程式化）或者稍後的時間。

【0104】 在決定步驟704，UE 102決定其是否已具有在供應的時候被初始化的PM SI。這可以例如在處理器202、記憶體204和PM SI模組208之間的合作下完成。若PM SI已被初始化，則方法700行進到步驟716，其中在步驟716，儲存初始PM SI並且PM SI初始化方法700結束。若PM SI尚未被初始化，則方法700行進到步驟706。

【0105】 在步驟706，處理器202和PM SI模組208一起合作並產生建議的初始PM SI。該建議的初始PM SI可以基於各種因素。在一個實施例中，該建議的初始PM SI可以基於UE 102的IMSI，例如基於結合亂數或偽亂數的一或多個散列函數及/或迭代。在另一個實施例中，PM SI未基於UE 102的IMSI，而是基於亂數或偽亂數（僅舉幾個例子），使得任何竊聽者將無法根據PM SI來推導IMSI。

【0106】 在步驟708，處理器202和PM SI模組208一起合作並對在步驟706處產生的該建議的初始PM SI進行加密。在一個實施例中，PM SI是使用伺服器112在先前一些時間與UE 102共享的公共金鑰來加密的。伺服器

112具有用於在接收時對PMSI進行解密的相應私密金鑰。

【0107】 在步驟710，UE 102例如經由基地台104及/或MME 106，經由收發機210向伺服器112發送經加密的PMSI。

【0108】 在步驟712，UE 102（經由收發機210）從伺服器112接收用於確認對建議的初始PMSI的接收的回應。

【0109】 在決定步驟714，處理器202和PMSI模組208一起合作並決定從伺服器112接收的回應是否指示伺服器112接受了建議的初始PMSI。若該回應指示伺服器112接受了建議的初始PMSI，則方法700行進到步驟716，其中在步驟716，儲存初始PMSI並且方法700結束。若該回應指示伺服器112沒有接受建議的初始PMSI，則方法700返回到步驟706以產生與剛被拒絕的該建議的初始PMSI不同的、新的建議的初始PMSI。例如當存在該PMSI與（例如，在伺服器112的資料庫310中）已儲存的、另一個關聯的UE的任何其他PMSI之間的衝突時，該建議的初始PMSI可能被拒絕。

【0110】 方法700可以重複進行直到得出UE 102和伺服器112均同意的PMSI為止。在替代的實施例中，若在決定步驟714處UE 102決定伺服器112沒有接受建議的初始PMSI，則UE 102亦可以查看來自伺服器112的回應（與步驟712處相同或不同的回應），以標識伺服器112

是否針對 UE 102 發送其自身建議的初始 PMSI。在該實施例中，UE 102 可以檢查來自伺服器 112 的該建議的初始 PMSI 以決定其對於 UE 102 是否是可接受的。不出任何問題的話，UE 102 可以接受來自伺服器 112 的該建議的初始 PMSI 並且向伺服器 112 通知該接受。一旦商定了初始 PMSI，就在 UE 102 處儲存該初始 PMSI 以供後續使用，並且方法 700 在步驟 716 處結束。

【0111】 圖 7B 是根據本案內容的各個態樣，圖示用於關於伺服器的使用 PMSI 的附著程序的示例性方法 720 的流程圖。出於簡化論述起見，將關於單個伺服器 112 和單個 UE 102 來描述方法 720，但是將認識到，本文所描述的態樣可以適用於任意數量的伺服器 112 及 / 或 UE 102。應當理解，可以在方法 720 的步驟之前、期間和之後提供額外的步驟，並且對於方法 720 的其他實施例來說可以替換或消除所描述的步驟中的一些步驟。

【0112】 在步驟 722，伺服器 112 例如經由收發機 312 從 UE 102 接收經加密的、建議的初始 PMSI。

【0113】 在步驟 724，例如經由處理器 302、記憶體 304 和 PMSI 模組 308 相合作，伺服器 112 解密所接收的 PMSI。在一個實施例中，所接收的 PMSI 是利用 UE 102 處的公共金鑰（其與在伺服器 112 處保持的私密金鑰或用於伺服器 112 的私密金鑰相對應）來加密的。

【0114】 在步驟 726，伺服器 112 將所接收的經解密的 PMSI 與資料庫 310 處（或伺服器 112 處的任何其他資料

庫中，或在保存用於複數個UE的資訊並可由伺服器112存取的別處）已存在的用於其他UE的其他PMSI值進行比較。

【0115】 在步驟728，伺服器112決定是否存在在所接收的、建議的初始PMSI與所儲存的或以其他方式可由伺服器112存取的任何其他PMSI值之間的任何衝突。

【0116】 在決定步驟730，基於在步驟728的決定結果，伺服器112決定是否接受該建議的初始PMSI。若伺服器112接受該建議的初始PMSI，則方法720行進到步驟734，其中在步驟734，伺服器112向UE 102發送對初始PMSI的接受確認，並且在伺服器112處將該初始PMSI儲存在資料庫310中，使得該初始PMSI與UE 102相關聯（例如，作為伺服器112為UE 102保持的記錄的一部分）。

【0117】 若在決定步驟730，伺服器112決定其不接受建議的初始PMSI，則方法720行進到步驟732，其中在步驟732，伺服器112從UE 102請求新的PMSI，伺服器112向UE 102發送請求並等待回應。在替代的實施例中，伺服器112可以替代地自己（on its own accord）產生建議的初始PMSI（回應於決定步驟730），並將該建議的初始PMSI與拒絕一起發送給UE 102。

【0118】 資訊和信號可以使用多種不同的技術和技藝中的任何技術和技藝來表示。例如，在貫穿上面的描述中可能提及的資料、指令、命令、資訊、信號、位元、符號

和碼片可以用電壓、電流、電磁波、磁場或粒子、光場或粒子或者其任意組合來表示。

【0119】 可以利用被設計為執行本文中所描述功能的通用處理器、DSP、ASIC、FPGA或其他可程式化邏輯裝置、個別閘門或者電晶體邏輯裝置、個別硬體元件或者其任意組合，來實現或執行結合本文揭示內容所描述的各種示例性框和模組。通用處理器可以是微處理器，或者，該處理器亦可以是任何一般的處理器、控制器、微控制器或者狀態機。處理器亦可以實現為計算設備的組合（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核心的結合，或者任何其他此種結構）。

【0120】 本文所描述的功能可以在硬體、由處理器執行的軟體、韌體，或其任意組合中實現。若在由處理器執行的軟體中實現，則該等功能可以作為一或多個指令或代碼儲存在電腦可讀取媒體上或經由其進行傳輸。其他例子和實現落在本案內容和所附申請專利範圍的保護範圍內。例如，由於軟體的本質，上文所描述的功能可以使用由處理器執行的軟體、硬體、韌體、硬佈線，或任意該等部件的組合來實現。用於實現功能的特徵亦可以實體地位於各種位置，包括被分佈為使得在不同的實體位置處實現功能的一部分。此外，如本文所使用的（包括在申請專利範圍中），如在項目列表（例如，以諸如「中的至少一個」或「中的一或多個」之類的短語為結束的項目列表）中所使用的「或」指示包含性列表，使得例如列表[A、B或C中

的至少一個]意指 A 或 B 或 C 或 A B 或 A C 或 B C 或 A B C (亦即, A 和 B 和 C)。

【0121】 本案內容的實施例包括一種使用者裝備 (UE), 該 UE 包括: 用於利用初始附著訊息, 向服務網路發送私密性行動用戶身份 (PM SI), 以替代國際行動用戶識別 (IM SI) 來標識該 UE 的手段; 用於從該服務網路接收認證請求的手段, 該認證請求包括由與該服務網路進行通訊的伺服器決定的下一個 PM SI, 該下一個 PM SI 是根據該 PM SI 來推導出的; 及用於經由該服務網路向該伺服器發送對該下一個 PM SI 的接收確認的手段。

【0122】 該 UE 亦包括: 用於根據先前的 PM SI 來推導該 PM SI 的手段, 其中該先前的 PM SI 包括初始 PM SI。該 UE 亦包括: 用於根據先前的 PM SI 來推導該 PM SI 的手段, 其中該先前的 PM SI 包括根據初始 PM SI 來推導的 PM SI 值。該 UE 亦包括: 用於由該 UE 基於初始 PM SI 來決定用於網路存取的該 PM SI 的手段。該 UE 亦包括: 用於在該 UE 向該伺服器進行用戶註冊的期間, 接收該初始 PM SI 的手段。該 UE 亦包括: 用於在經由空中通訊向該伺服器進行用戶註冊之後, 供應該初始 PM SI 的手段。該 UE 亦包括: 用於產生建議的 PM SI 的手段; 用於使用伺服器公共金鑰來加密所產生的 PM SI 的手段, 其中該伺服器保存相應的伺服器私密金鑰; 及用於從該伺服器接收要使用所產生的 PM SI 作為該初始 PM SI 的確認的手段。該 UE 亦包括: 用於決定基於 UE 的下一個 PM SI 的手段; 及

用於將該基於UE的下一個PMSI與作為該認證請求的一部分而接收的該下一個PMSI進行比較，以決定是否存在匹配的手段。該UE亦包括：用於回應於決定存在匹配，產生確認符記的手段，該接收確認包括該確認符記；及用於在該UE處儲存所確認的下一個PMSI以用於下一個附著訊息中的手段。該UE亦包括：用於使用匿名金鑰來解密該認證請求中的該下一個PMSI的手段，其中該匿名金鑰是根據在該UE與該伺服器之間共享的秘密金鑰來推導出的。

【0123】 本案內容的實施例亦包括一種伺服器，該伺服器包括：用於經由中間服務網路中的一或多個網路單元，經由初始附著訊息來從使用者裝備（UE）接收私密性行動用戶身份（PMSI），以替代國際行動用戶識別（IMSI）來標識該UE的手段；用於由該伺服器基於該PMSI來決定下一個PMSI的手段；用於從該伺服器向該服務網路發送包括該下一個PMSI的認證資訊的手段，其中作為認證的一部分，該下一個PMSI由該服務網路中繼給該UE；及用於經由該服務網路從該UE接收包括對該下一個PMSI的確認的接收確認的手段。

【0124】 該伺服器亦包括：用於根據先前的PMSI來推導該下一個PMSI的手段，其中該先前的PMSI包括初始PMSI。該伺服器亦包括：用於根據先前的PMSI來推導該下一個PMSI的手段，其中該先前的PMSI包括根據初始PMSI來推導的PMSI值。該伺服器亦包括：用於由該

伺服器基於初始 P M S I 來決定用於網路存取的該 P M S I 的手段。該伺服器亦包括：用於在該伺服器處，在該 U E 向該伺服器進行用戶註冊的期間接收該初始 P M S I 的手段。該伺服器亦包括：用於從該 U E 接收建議的初始 P M S I 的手段；用於由該伺服器使用伺服器私密金鑰來解密在該 U E 處經由相應的伺服器公共金鑰來加密的該建議的初始 P M S I 的手段；及用於向該 U E 發送將該建議的初始 P M S I 作為該初始 P M S I 的確認的手段。該伺服器亦包括：用於根據在該伺服器與該 U E 之間共享的秘密金鑰來推導匿名金鑰的手段；用於使用所推導的匿名金鑰來加密該認證資訊中的該下一個 P M S I 的手段；用於作為該確認的一部分，接收對該下一個 P M S I 進行確認的確認符記的手段；及用於在該伺服器處儲存該下一個 P M S I 以替代該 P M S I，以用於回應來自該 U E 的後續初始附著訊息的手段。該伺服器亦包括：用於偵測該下一個 P M S I 與關聯於不同的 U E 的另一個現有 P M S I 之間的衝突的手段；及用於對 P M S I 索引進行遞增，並且基於該下一個 P M S I 和經遞增的 P M S I 索引來決定新的下一個 P M S I 的手段。該伺服器亦包括：用於從與該伺服器所位於的歸屬網路分開的該服務網路上的行動性管理實體（ M M E ）接收針對該 U E 的該 I M S I 的請求的手段；及用於回應於該請求，發送在該初始附著訊息中所使用的、該 U E 的該 P M S I 而不是該 U E 的該 I M S I 的手段。該伺服器亦包括：用於針對對利用該初始附著訊息包括的該 P M S I 的匹配，搜尋一或多個

資料庫的手段；及用於回應於沒有定位到匹配，發送針對該 UE 的通知來修改在該 UE 處保存的 P M S I 索引以便在該 UE 處產生經更新的 P M S I 的手段。

【0125】 本案內容的實施例亦包括一種用於由使用者裝備（UE）進行的網路存取的方法，該方法包括：由該 UE 決定在服務網路處進行附著；及從該 UE 向該服務網路發送初始附著訊息，該初始附著訊息包括臨時識別符（ID）以替代用於該 UE 的永久 ID，其中基於該臨時 ID 來建立與該服務網路的認證伺服器（HSS）的安全上下文。

【0126】 該方法亦包括：從該服務網路的該 HSS 接收認證請求，該認證請求包括由該 HSS 決定的下一個臨時 ID，該下一個臨時 ID 是根據該初始附著訊息中所包括的該臨時 ID 來推導出的。該方法亦包括：從該 UE 經由該服務網路向該 HSS 發送對該下一個臨時 ID 的接收確認。

【0127】 本案內容的實施例亦包括一種使用者裝備，該使用者裝備包括：記憶體，其被配置為儲存臨時識別符（ID）；處理器，其被配置為決定在服務網路處進行附著；及收發機，其被配置為向該服務網路發送初始附著訊息，該初始附著訊息包括臨時 ID 以替代用於該 UE 的永久 ID，其中與該服務網路的認證伺服器（HSS）的安全上下文是基於該臨時 ID 來建立的。

【0128】 該 UE 亦包括：其中該收發機亦被配置為從該服務網路的該 HSS 接收認證請求，該認證請求包括由該

HSS 決定的下一個臨時ID，該下一個臨時ID是根據該初始附著訊息中所包括的該臨時ID來推導出的。該UE亦包括：其中該處理器亦被配置為產生接收確認，並且該收發機亦被配置為經由該服務網路向該HSS發送該接收確認。

【0129】 本案內容的實施例亦包括一種用於與網路上的伺服器建立網路存取的方法，該方法包括：經由服務網路從使用者裝備（UE）接收初始附著訊息，該初始附著訊息包括臨時識別符（ID）以替代用於該UE的永久ID；及基於該臨時ID來建立安全上下文。

【0130】 該方法亦包括：基於該初始附著訊息中所包括的該臨時ID來決定下一個臨時ID。該方法亦包括：作為認證的一部分，從該伺服器經由該服務網路向該UE發送包括該下一個臨時ID的認證資訊。該方法亦包括：經由該服務網路從該UE接收包括對該下一個臨時ID的確認的接收確認。

【0131】 本案內容的實施例亦包括一種伺服器，該伺服器包括：收發機，其被配置為經由服務網路從使用者裝備（UE）接收初始附著訊息，該初始附著訊息包括臨時識別符（ID）以替代用於該UE的永久ID；及處理器，其被配置為基於該臨時ID來建立安全上下文。

【0132】 該伺服器亦包括：其中該處理器亦被配置為基於該初始附著訊息中所包括的該臨時ID來決定下一個臨時ID。該伺服器亦包括：其中該收發機亦被配置為：作

為認證的一部分，經由該服務網路向該UE發送包括該下一個臨時ID的認證資訊。該伺服器亦包括：其中該收發機亦被配置為經由該服務網路從該UE接收包括對該下一個臨時ID的確認的接收確認。

【0133】如本領域技藝人士到目前為止將意識到的，並且取決於手邊的特定應用，可以在使用本案內容的設備的材料、裝置、配置和方法中或對使用本案內容的設備的材料、裝置、配置和方法進行許多種修改、替換和變更。鑒於這一點，本案內容的範圍不應受限於本文示出和描述的特定實施例，因為該等特定實施例是僅經由其一些例子來舉例說明的，而是相反地，該範圍應與所附申請專利範圍及其功能均等物的範圍完全相稱。

【符號說明】

【0134】

100 無線通訊網路

102 UE

104 基地台

106 行動性管理實體（MME）

108 服務網路

110 網路

112 伺服器

114 歸屬網路

202 處理器

- 2 0 4 記 憶 體
- 2 0 6 指 令
- 2 0 8 P M S I 模 組
- 2 1 0 收 發 機
- 2 1 2 數 據 機 子 系 統
- 2 1 4 射 頻 (R F) 單 元
- 2 1 6 天 線
- 3 0 2 處 理 器
- 3 0 4 記 憶 體
- 3 0 6 指 令
- 3 0 8 P M S I 模 組
- 3 1 0 資 料 庫
- 3 1 2 收 發 機
- 4 0 0 M I M O 系 統
- 4 1 0 示 例 性 發 射 器 系 統
- 4 1 2 資 料 來 源
- 4 1 4 發 射 (T X) 資 料 處 理 器
- 4 2 0 T X M I M O 處 理 器
- 4 2 2_a 發 射 器 (T M T R)
- 4 2 2_t 發 射 器 (T M T R)
- 4 2 4_a 天 線
- 4 2 4_t 天 線
- 4 3 0 處 理 器
- 4 3 2 記 憶 體

- 4 3 6 資 料 來 源
- 4 3 8 T X 資 料 處 理 器
- 4 4 0 解 調 器
- 4 4 2 R X 資 料 處 理 器
- 4 5 0 接 收 器 系 統
- 4 5 2_a 天 線
- 4 5 2_r 天 線
- 4 5 4_a 接 收 器 (R C V R)
- 4 5 4_r 接 收 器 (R C V R)
- 4 6 0 R X 資 料 處 理 器
- 4 7 0 處 理 器
- 4 7 2 記 憶 體
- 4 8 0 T X M I M O 處 理 器
- 5 0 2 動 作
- 5 0 8 動 作
- 5 1 4 動 作
- 5 1 8 動 作
- 6 0 0 示 例 性 方 法
- 6 0 2 步 驟
- 6 0 4 步 驟
- 6 0 6 步 驟
- 6 0 8 步 驟
- 6 1 0 步 驟
- 6 1 2 步 驟

6 1 4 決 定 步 驟

6 1 6 步 驟

6 1 8 步 驟

6 2 0 步 驟

6 3 0 示 例 性 方 法

6 3 2 步 驟

6 3 4 步 驟

6 3 6 步 驟

6 3 8 步 驟

6 4 0 決 定 步 驟

6 4 2 步 驟

6 4 4 步 驟

6 4 6 步 驟

7 0 0 示 例 性 方 法

7 0 2 步 驟

7 0 4 決 定 步 驟

7 0 6 步 驟

7 0 8 步 驟

7 1 0 步 驟

7 1 2 步 驟

7 1 4 決 定 步 驟

7 1 6 步 驟

7 2 0 示 例 性 方 法

7 2 2 步 驟

7 2 4 步 驟

7 2 6 步 驟

7 2 8 步 驟

7 3 0 決 定 步 驟

7 3 4 步 驟

【生物材料寄存】

【 0 1 3 5 】 國內寄存資訊 (請依寄存機構、日期、號碼順序註記)

無

【 0 1 3 6 】 國外寄存資訊 (請依寄存國家、機構、日期、號碼順序註

記)

無

【發明申請專利範圍】

【第1項】 一種用於無線通訊的方法，該方法包括以下步驟：

由一使用者裝備（UE）經由一空中連接向一歸屬網路發起註冊；

由該UE產生一建議的私密性行動用戶身份（PM-SI）以用作一國際行動用戶識別（IMSI）的一替代品；

由該UE經由該空中連接向該歸屬網路發送該建議的PM-SI；及

由該UE回應於從該歸屬網路接收指示該建議的PM-SI被接受的一確認訊息，將該建議的PM-SI用作於一附著訊息的一初始PM-SI以供向一服務網路發送。

【第2項】 如請求項1所述的方法，進一步包括以下步驟：

由該UE回應於指示該建議的PM-SI被拒絕的該確認訊息，重新產生一新建議的PM-SI；及

由該UE經由該空中連接向該歸屬網路重新發送該新建議的PM-SI。

【第3項】 如請求項1所述的方法，進一步包括以下步驟：

由該UE從該確認訊息存取一伺服器建議的PM-SI以替代該建議的PM-SI；及

由該 U E 向該歸屬網路通知該伺服器建議的 P M S I 被接受以用作該初始 P M S I 。

【第 4 項】 如請求項 1 所述的方法，其中該產生步驟進一步包括以下步驟：

由該 U E 基於一偽亂數來產生該建議的 P M S I 。

【第 5 項】 如請求項 1 所述的方法，其中該產生步驟進一步包括以下步驟：

由該 U E 基於該 I M S I 來產生該建議的 P M S I 。

【第 6 項】 如請求項 1 所述的方法，進一步包括以下步驟：

由該 U E 在該發送步驟之前從該歸屬網路接收一公共金鑰；及

由該 U E 在該發送步驟之前用該公共金鑰加密該建議的 P M S I 。

【第 7 項】 如請求項 1 所述的方法，進一步包括以下步驟：

由該 U E 回應於該附著訊息從該服務網路接收一認證請求，該認證請求包括一下一個 P M S I 及一追蹤索引；

由該 U E 將該下一個 P M S I 與一 U E 推導的下一個 P M S I 進行比較；及

由該 U E 向該服務網路確認該下一個 P M S I 以用於一後續的附著訊息中。

【第 8 項】 一種使用者裝備，包括：

一處理器，被配置為產生一建議的私密性行動用戶身份（PMSI）以用作一國際行動用戶識別（IMSI）的一替代品；及

一收發機，被配置為：

經由一空中連接向一歸屬網路發起註冊；及

經由該空中連接向該歸屬網路發送該建議的PMSI，其中該處理器被進一步配置為回應於從該歸屬網路接收指示該建議的PMSI被接受的一確認訊息，將該建議的PMSI用作用於一附著訊息的一初始PMSI。

【第9項】 如請求項8所述的使用者裝備，其中：

該處理器被進一步配置為回應於指示該建議的PMSI被拒絕的該確認訊息，重新產生一新建議的PMSI；及

該收發機被進一步配置為經由該空中連接向該歸屬網路重新發送該新建議的PMSI。

【第10項】 如請求項8所述的使用者裝備，其中：

該處理器被進一步配置為從該確認訊息存取一伺服器建議的PMSI以替代該建議的PMSI；及

該收發機被進一步配置為向該歸屬網路通知該伺服器建議的PMSI被接受以用作該初始PMSI。

【第11項】 如請求項8所述的使用者裝備，其中該處理器被進一步配置為作為該產生步驟的一部分，基於一偽亂數來產生該建議的PMSI。

【第12項】 如請求項8所述的使用者裝備，其中該處理器被進一步配置為作為該產生步驟的一部分，基於該IMSI來產生該建議的PM SI。

【第13項】 如請求項8所述的使用者裝備，其中：

該收發機被進一步配置為在該發送步驟之前從該歸屬網路接收一公共金鑰；及

該處理器被進一步配置為在該發送步驟之前用該公共金鑰加密該建議的PM SI。

【第14項】 如請求項8所述的使用者裝備，其中：

該收發機被進一步配置為向一服務網路以該附著訊息發送用於識別該UE的該初始PM SI；

該收發機被進一步配置為回應於該附著訊息從該服務網路接收一認證請求，該認證請求包括一下一個PM SI及一追蹤索引；

該處理器被進一步配置為將該下一個PM SI與一UE推導的下一個PM SI進行比較；及

該收發機被進一步配置為向該服務網路確認該下一個PM SI以用於一後續的附著訊息中。

【第15項】 一種非暫時性電腦可讀取媒體，該非暫時性電腦可讀取媒體上記錄有程式碼，該程式碼包括：

用於使一使用者裝備（UE）經由一空中連接向一歸屬網路發起註冊的代碼；

用於使該 UE 產生一建議的私密性行動用戶身份 (PMSI) 以用作一國際行動用戶識別 (IMSI) 的一替代品的代碼；

用於使該 UE 經由該空中連接向該歸屬網路發送該建議的 PMSI 的代碼；及

用於使該 UE 回應於從該歸屬網路接收指示該建議的 PMSI 被接受的一確認訊息，將該建議的 PMSI 用作用於一附著訊息的一初始 PMSI 的代碼。

【第 16 項】 如請求項 15 所述的非暫時性電腦可讀取媒體，進一步包括：

用於使該 UE 回應於指示該建議的 PMSI 被拒絕的該確認訊息，重新產生一新建議的 PMSI 的代碼；及

用於使該 UE 經由該空中連接向該歸屬網路重新發送該新建議的 PMSI 的代碼。

【第 17 項】 如請求項 15 所述的非暫時性電腦可讀取媒體，進一步包括：

用於使該 UE 從該確認訊息存取一伺服器建議的 PMSI 以替代該建議的 PMSI 的代碼；及

用於使該 UE 向該歸屬網路通知該伺服器建議的 PMSI 被接受以用作該初始 PMSI 的代碼。

【第 18 項】 如請求項 15 所述的非暫時性電腦可讀取媒體，其中該用於造成該產生步驟的代碼進一步包括：

用於使該 UE 基於一偽亂數來產生該建議的 PMSI 的代碼。

【第19項】 如請求項15所述的非暫時性電腦可讀取媒體，進一步包括：

用於使該UE在該發送步驟之前從該歸屬網路接收一公共金鑰的代碼；及

用於使該UE在該發送步驟之前用該公共金鑰加密該建議的PMSE的代碼。

【第20項】 如請求項15所述的非暫時性電腦可讀取媒體，進一步包括：

用於使該UE向一服務網路以該附著訊息發送用於識別該UE的該初始PMSE的代碼；

用於使該UE回應於該附著訊息從該服務網路接收一認證請求的代碼，該認證請求包括一下一個PMSE及一追蹤索引；

用於使該UE將該下一個PMSE與一UE推導的下一個PMSE進行比較的代碼；及

用於使該UE向該服務網路確認該下一個PMSE以用於一後續的附著訊息中的代碼。

【發明圖式】

100

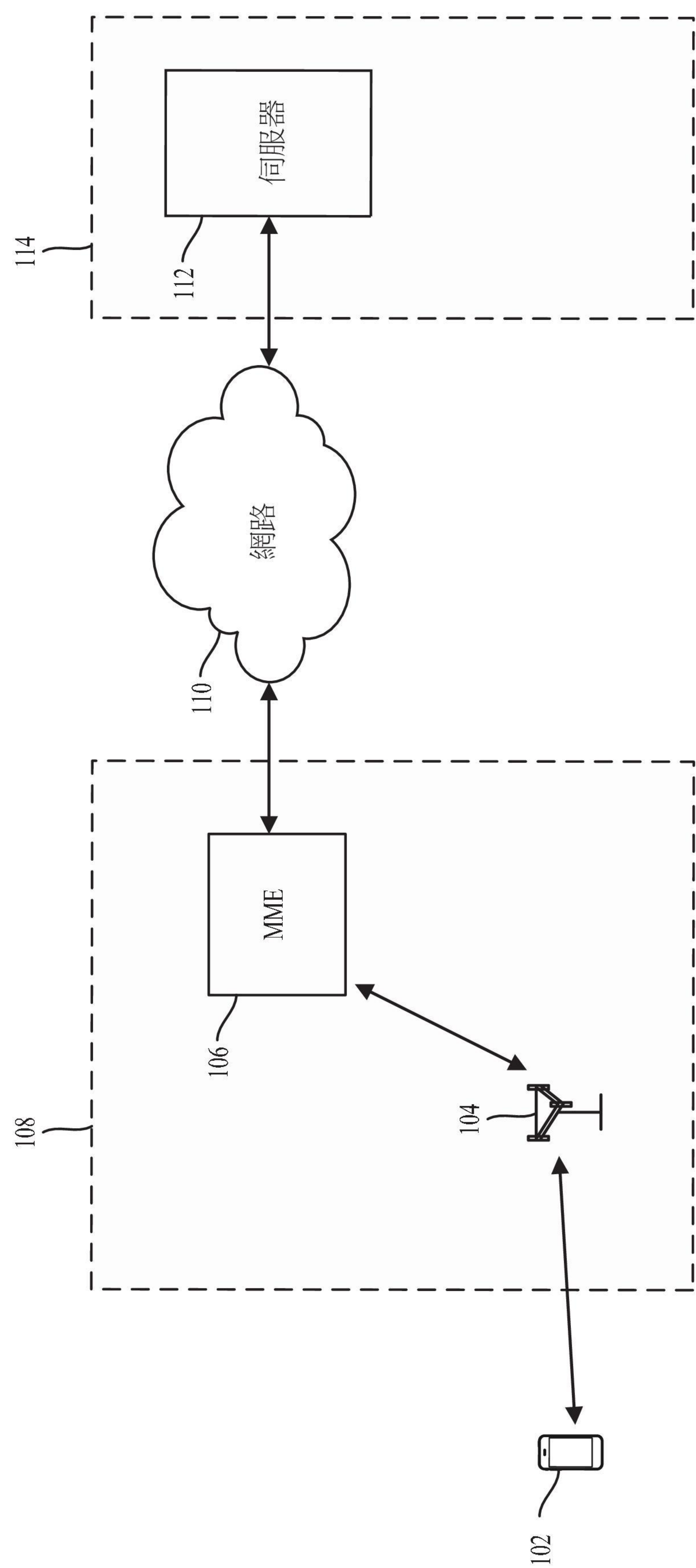


圖1

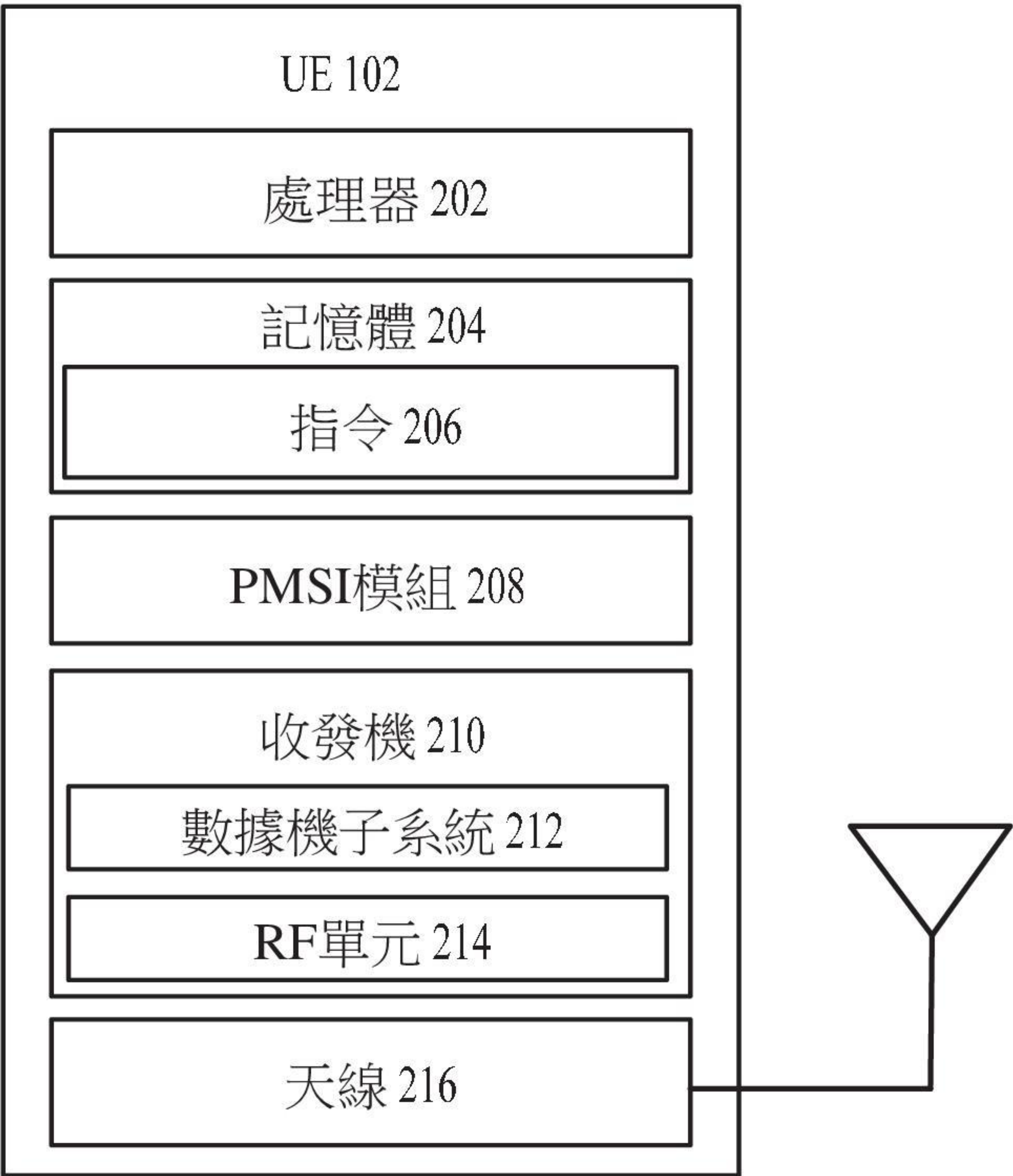


圖2



圖3

400

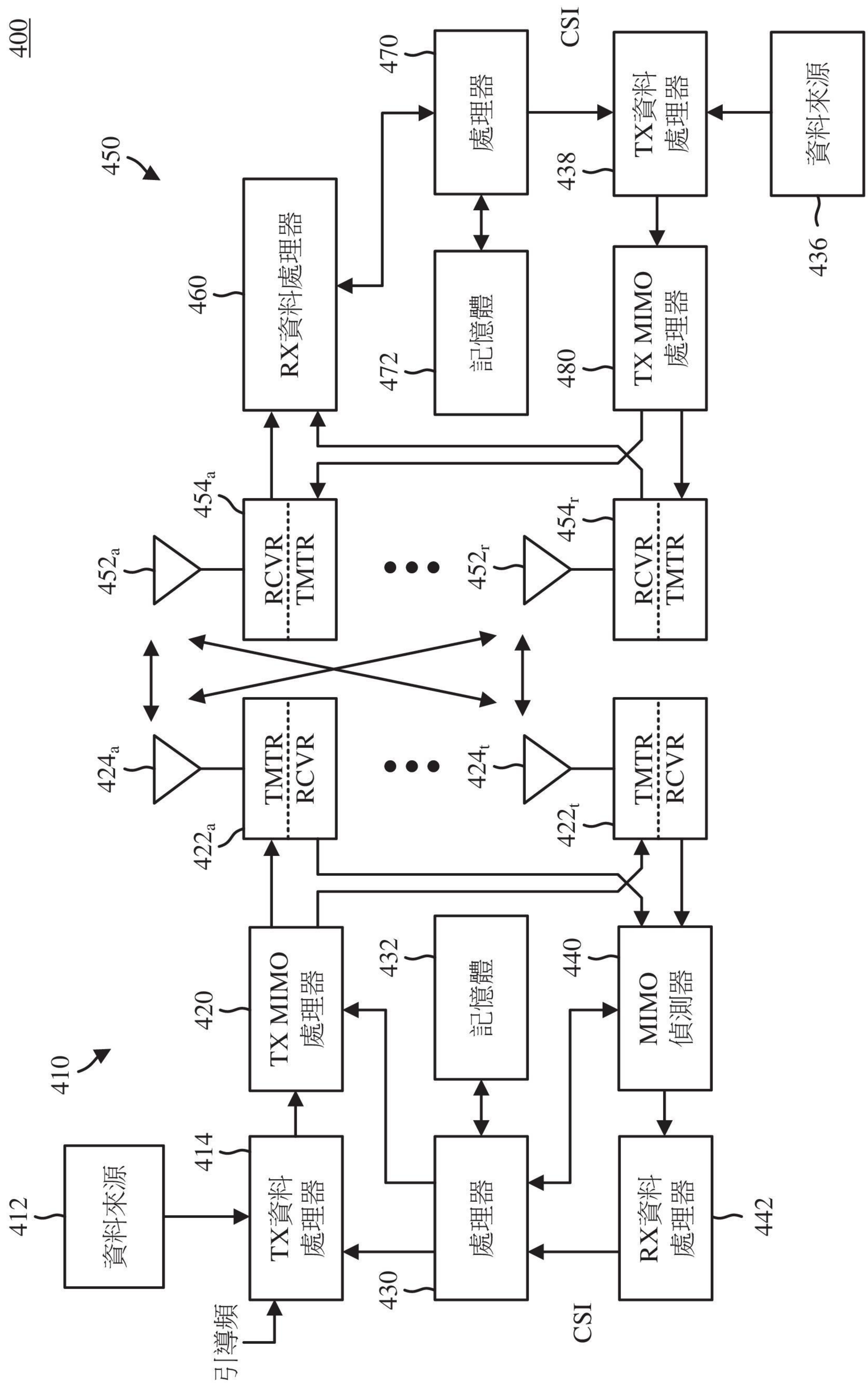


圖4

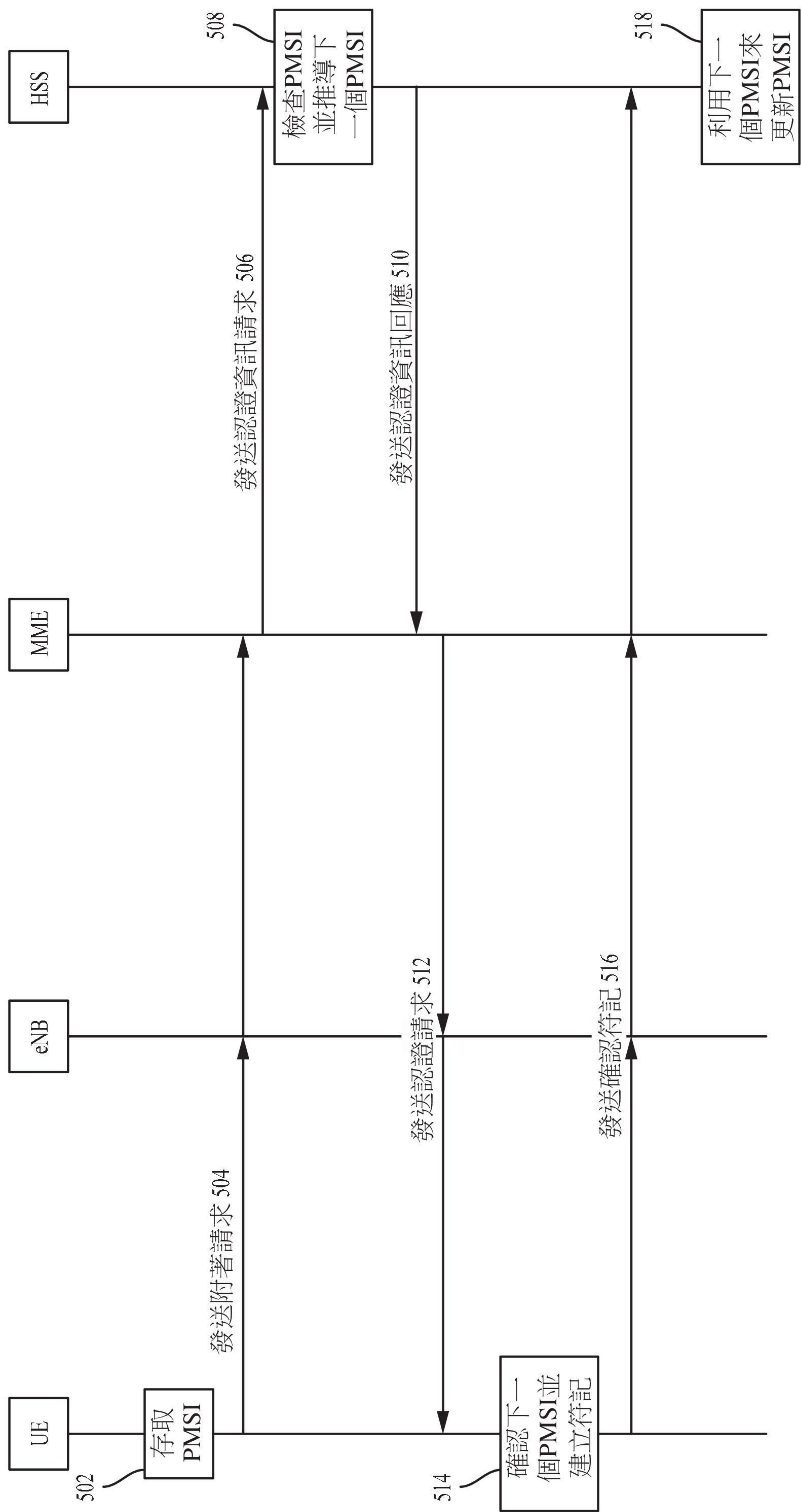


圖5

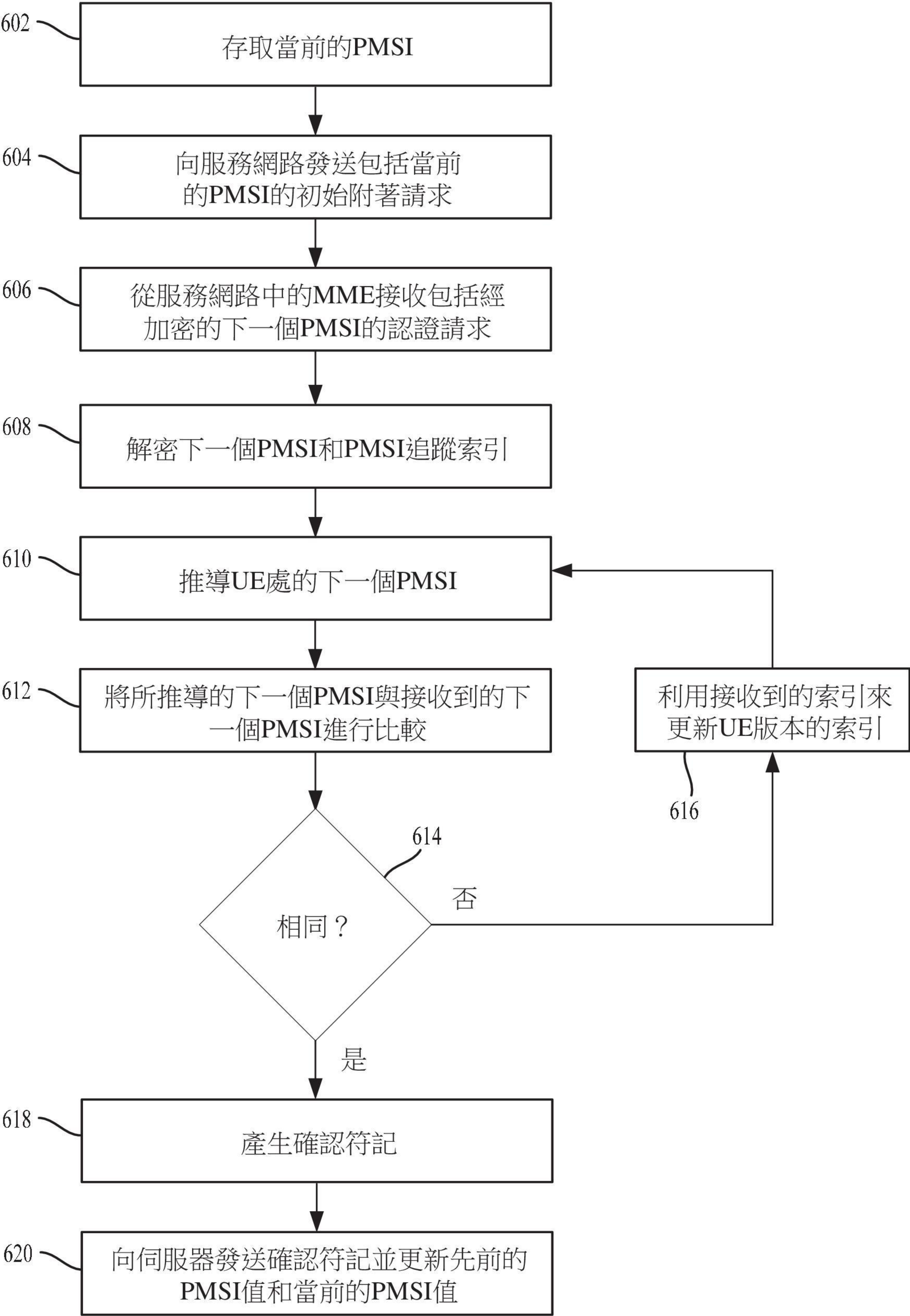


圖6A

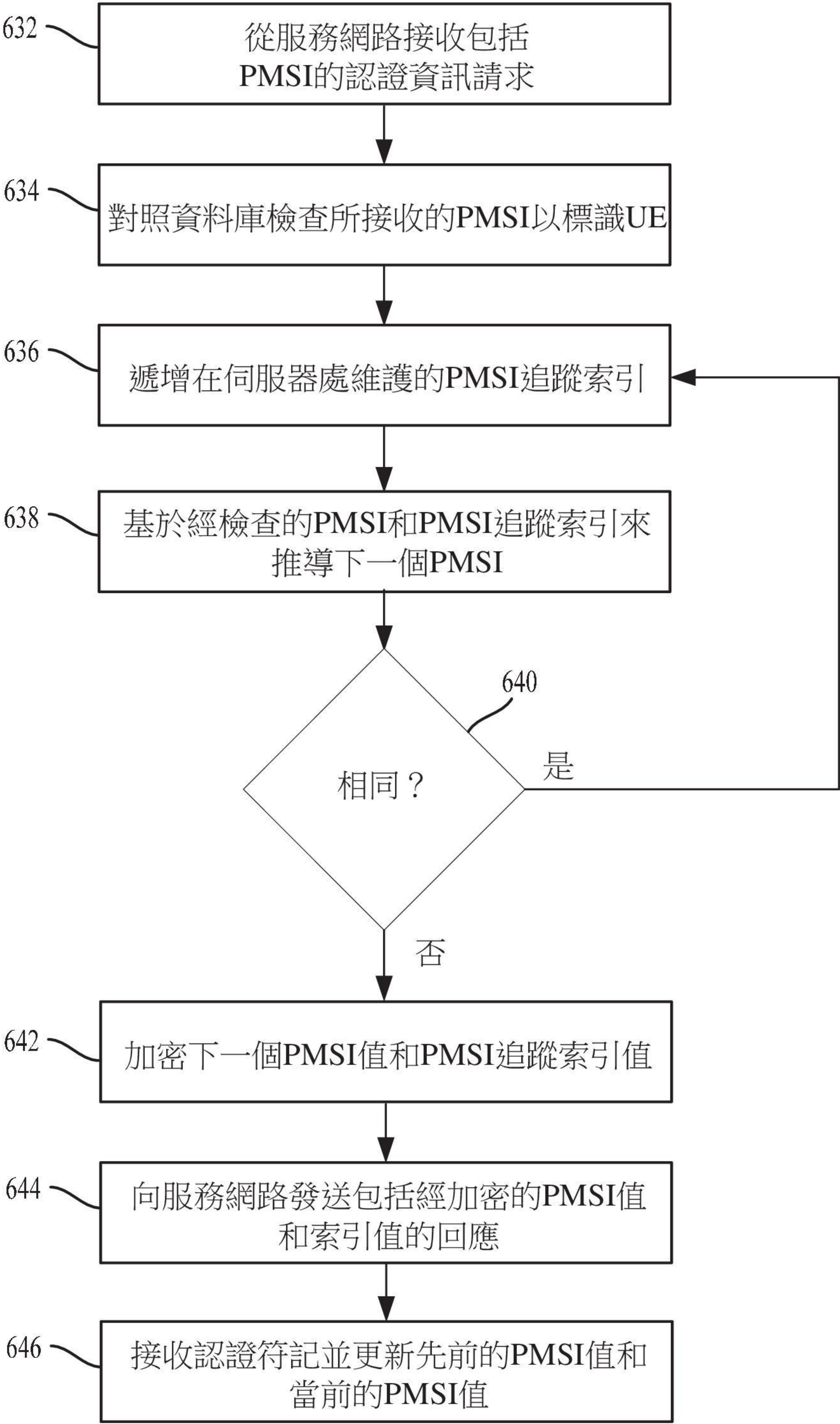


圖6B

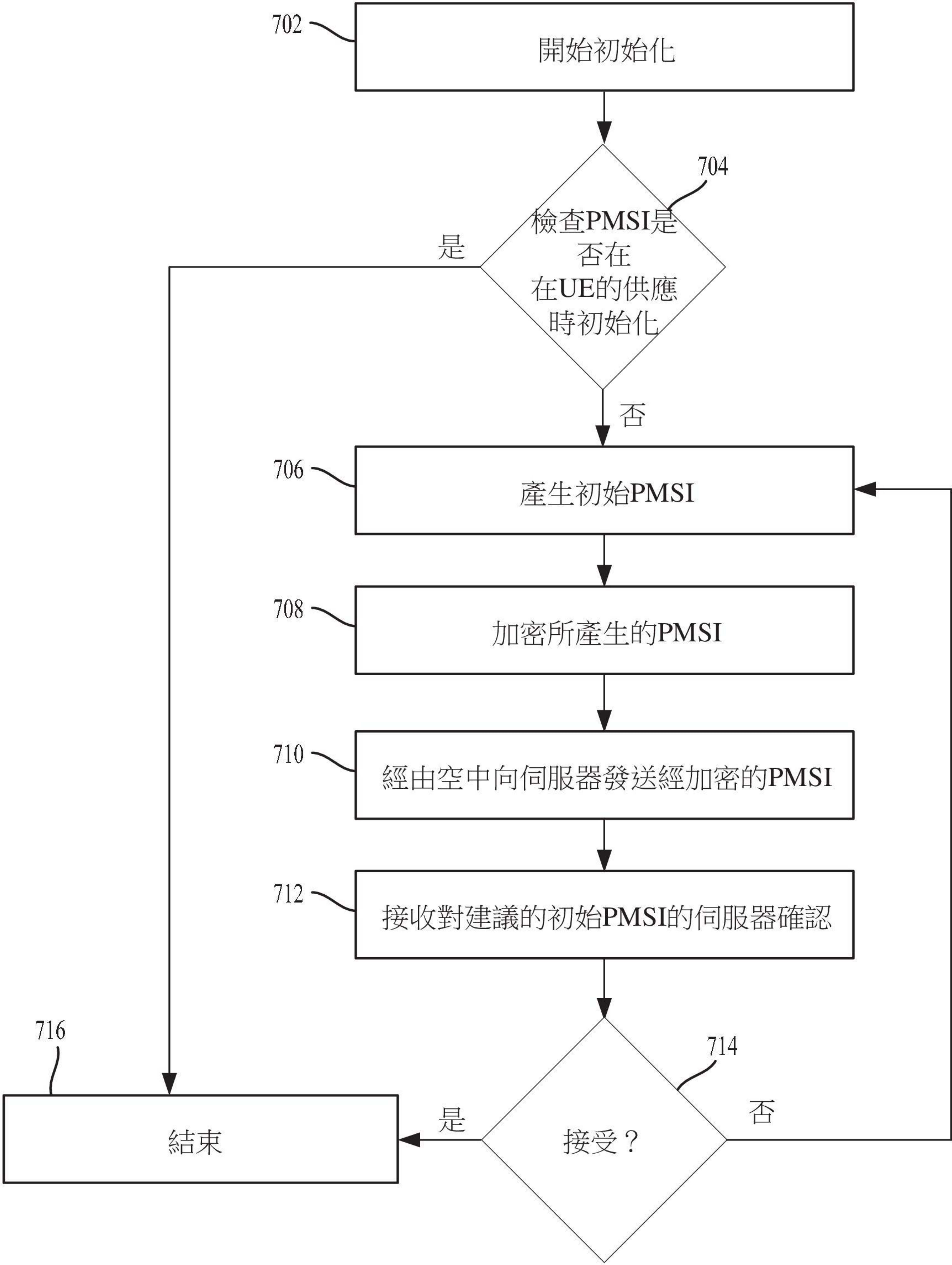


圖7A

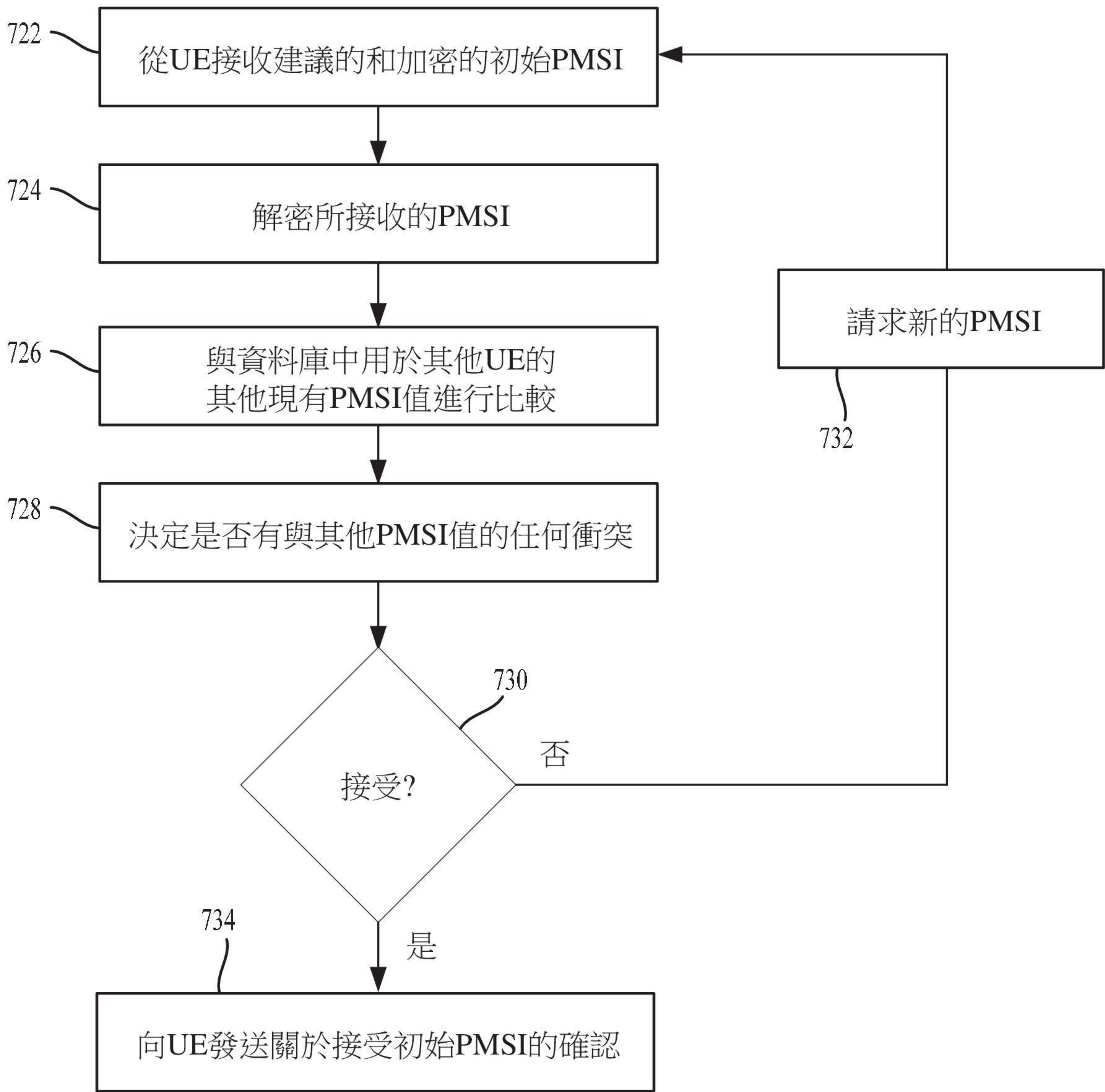


圖7B