



(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 201626751 A

(43)公開日：中華民國 105 (2016) 年 07 月 16 日

(21)申請案號：104127970

(22)申請日：中華民國 104 (2015) 年 08 月 26 日

(51)Int. Cl. : *H04L9/08 (2006.01)* *H04W12/04 (2009.01)*

(30)優先權：2014/09/26 美國 62/056,371

2015/03/31 美國 14/674,763

(71)申請人：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)；霍恩蓋文 HORN, GAVIN (US)

(74)代理人：李世章

申請實體審查：無 申請專利範圍項數：29 項 圖式數：17 共 74 頁

(54)名稱

服務網路認證

SERVING NETWORK AUTHENTICATION

(57)摘要

提供了用於無線通訊的一種方法、裝置和電腦程式產品。該方法可以包括：建立與服務網路的連接；向該服務網路發送加密的認證憑證，該認證憑證包括隨機選擇的金鑰加密金鑰(KEK)和服務網路辨識符；接收來自於該服務網路的認證資訊和簽名；及經由基於該 KEK 驗證簽名，來認證該服務網路。該加密的認證憑證可以可操作以辨識該服務網路。該簽名可以使用 KEK 來產生。

A method, an apparatus, and a computer program product for wireless communication are provided. The method may include establishing a connection with a serving network, transmitting an encrypted authentication credential that includes a randomly selected key encryption key (KEK) and a serving network identifier to the serving network, receiving authentication information and a signature from the serving network, and authenticating the serving network by verifying the signature based on the KEK. The encrypted authentication credential may be operative to identify the serving network. The signature may be generated using the KEK.

指定代表圖：

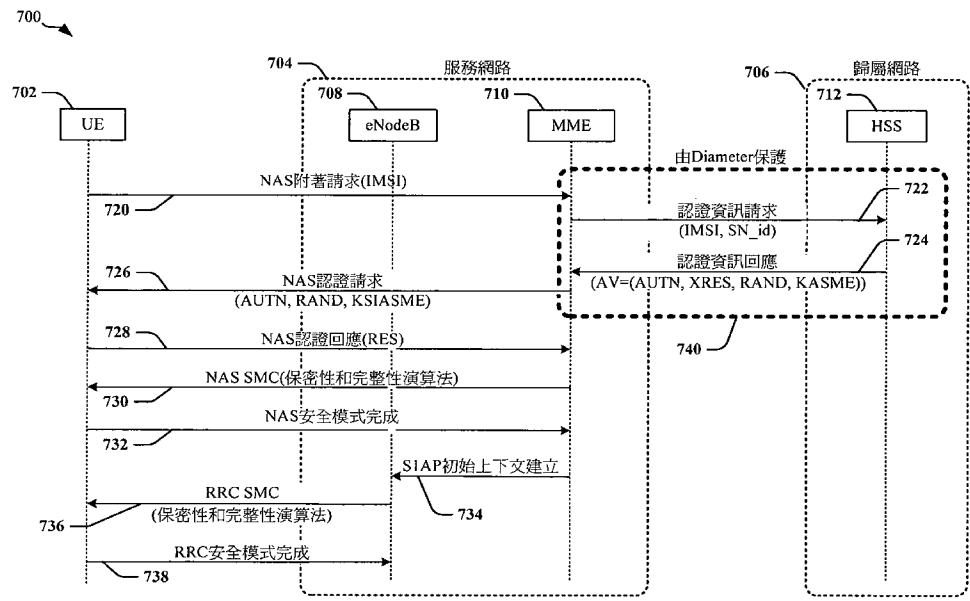


圖 7

- 符號簡單說明：
- 700 . . . 訊息流程圖
 - 702 . . . UE
 - 704 . . . 服務網路
 - 706 . . . 歸屬網路
 - 708 . . . eNodeB
 - 710 . . . MME
 - 712 . . . HSS
 - 720 . . . NAS 附着請求
 - 722 . . . NAS 附着請求
 - 724 . . . 認證資訊回應訊息
 - 726 . . . NAS 認證請求
 - 728 . . . NAS 認證回應訊息
 - 730 . . . 非存取層(NAS)安全模式配置(NAS SMC)訊息
 - 732 . . . 「NAS 安全模式完成」訊息
 - 734 . . . 「SIAP 初始上下文建立」訊息
 - 736 . . . RRC 非存取層(NAS)安全模式配置(RRC SMC)訊息
 - 738 . . . RRC 安全模式完成訊息
 - 740 . . . 鏈路

發明摘要

※ 申請案號：104127970

※ 申請日：2015 年 8 月 26 日

※IPC 分類：

H04L 9/08

(2006.01)

H04L 12/04

(2009.01)

【發明名稱】（中文/英文）

服務網路認證

SERVING NETWORK AUTHENTICATION

【中文】

提供了用於無線通訊的一種方法、裝置和電腦程式產品。該方法可以包括：建立與服務網路的連接；向該服務網路發送加密的認證憑證，該認證憑證包括隨機選擇的金鑰加密金鑰（KEK）和服務網路辨識符；接收來自於該服務網路的認證資訊和簽名；及經由基於該KEK驗證簽名，來認證該服務網路。該加密的認證憑證可以可操作以辨識該服務網路。該簽名可以使用KEK來產生。

【英文】

A method, an apparatus, and a computer program product for wireless communication are provided. The method may include establishing a connection with a serving network, transmitting an encrypted authentication credential that includes a randomly selected key encryption key (KEK) and a serving network identifier to the serving network, receiving authentication information and a signature from the serving network, and authenticating the serving

network by verifying the signature based on the KEK. The encrypted authentication credential may be operative to identify the serving network. The signature may be generated using the KEK.

【代表圖】

【本案指定代表圖】：第（ 7 ）圖。

【本代表圖之符號簡單說明】：

700 訊息流程圖

702 UE

704 服務網路

706 歸屬網路

708 eNodeB

710 MME

712 HSS

720 NAS 附著請求

722 NAS 附著請求

724 認證資訊回應訊息

726 NAS 認證請求

728 NAS 認證回應訊息

730 非存取層（NAS）安全模式配置（NAS SMC）訊息

732 「NAS 安全模式完成」訊息

734 「S1AP 初始上下文建立」訊息

736 RRC 非存取層（NAS）安全模式配置（RRC SMC）
訊息

738 RRC 安全模式完成訊息

740 鏈路

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

服務網路認證

SERVING NETWORK AUTHENTICATION

【對相關申請案的交叉引用】

【0001】本專利申請案主張2014年9月26日於美國專利和商標局遞交的臨時申請案第62/056,371號的優先權和權益以及非臨時申請案第14/674,763號的優先權和權益，經由引用方式將以上申請案的全部內容併入本文。

【技術領域】

【0002】概括地說，本案內容係關於通訊系統，並且更具體地說，係關於用於在無線通訊系統中在使用者設備和服務網路之間進行認證的系統。

【先前技術】

【0003】為了提供諸如語音、視訊、資料、訊息傳遞和廣播等各種電信服務，廣泛地布署了無線通訊系統。典型的無線通訊系統可以使用能夠經由共用可用的系統資源（例如，頻寬、傳輸功率）來支援與多個使用者通訊的多工存取技術。這種多工存取技術的例子係包括分碼多工存取（CDMA）系統、分時多工存取（TDMA）系統、分頻多工存取（FDMA）系統、正交分頻多工存取（OFDMA）系統、單載波分頻多工存取（SC-FDMA）系統、和分時同步分碼多工存取（TD-SCDMA

）系統。

【0004】在各種電信標準中已經採用了這些多工存取技術以提供使得不同的無線設備能在城市、國家、地區乃至全球層面進行通訊的公共協定。隨著多工存取技術的提高和增強，出現了新的電信標準。新興電信標準的例子是第四代長期進化（LTE）。LTE是對由第三代合作夥伴計畫（3GPP）頒佈的通用行動電信系統（UMTS）行動服務標準的增強集。它被設計用於經由以下行為來更好地支援行動寬頻網際網路存取：提高頻譜效率、降低成本、改善服務、利用新的頻譜，以及經由在下行鏈路（DL）上使用OFDMA、在上行鏈路（UL）上使用SC-FDMA以及使用多輸入多輸出（MIMO）天線技術來與其他開放標準更好地整合。然而，隨著對行動寬頻存取的需求持續增加，存在對LTE技術的進一步改進的需求，及/或對具有提高的能力的新一代電信標準的需求。

【0005】安全配置是在LTE網路中建立邏輯承載或通道（例如，在行動通訊設備和網路實體或存取點之間的通訊鏈路）的初始步驟。金鑰推導和建立是該安全配置的一部分。產生的金鑰的大部分是用於非存取層（NAS）安全模式配置（NAS SMC）和存取層（AS）安全模式配置（AS SMC）的加密和完整性金鑰。隨著新一代通訊技術的布署，安全配置程序中可能會暴露針對攻擊的漏洞。因此，存在對改進安全性程序的需要。優選地，改進應當適用於其他的多工存取技術以及採用這些技術的電信標準。

【發明內容】

【0006】在本案內容的一個態樣，提供了一種方法、電腦程式產品和裝置。

【0007】根據某些態樣，一種用於在使用者設備（UE）處的無線通訊的方法包括：建立與服務網路的連接；向該服務網路的網路節點發送包括認證憑證的第一訊息，該認證憑證包括隨機選擇的金鑰加密金鑰（KEK）和服務網路辨識符，其中該認證憑證是使用歸屬網路中的歸屬用戶伺服器（HSS）的加密金鑰來加密的；接收回應於該第一訊息的第二訊息，其中該第二訊息包括來自該網路節點的認證請求和由該網路節點使用該KEK產生的簽名；及基於該簽名來認證該網路節點。

【0008】根據某些態樣，一種用於服務網路中的行動性管理實體（MME）處的無線通訊的方法包括：接收來自UE的第一請求，該第一請求用於與該服務網路建立連接，該第一請求包括該UE的唯一辨識碼和加密的資訊。該加密的資訊包括該服務網路的辨識符和隨機選擇的金鑰加密金鑰（KEK），並且該方法亦包括：向與該UE相關聯的歸屬網路的HSS發送第二請求，該請求包括在該第一請求中接收到的該加密的資訊和該MME的公開金鑰。該方法亦包括：接收來自該HSS的對該第二請求的回應，對該第二請求的該回應包括使用該MME的公開金鑰加密的該KEK，以及使用該KEK加密的認證向量；使用與該MME的該公開金鑰相對應的私密金鑰來解密該KEK；使用該KEK來解密該認證向量；及向該UE發送第三請求，該第三請求包括使用該KEK簽名的認證請求。

【0009】根據某些態樣，一種用於UE的歸屬網路中的HSS處的無線通訊的方法包括：接收來自服務網路的節點的認證資訊請求，其中該請求包括第一服務網路辨識符、該服務網路的該節點的公開金鑰、以及由該UE加密的資訊。由該UE加密的該資訊包括隨機選擇的KEK和第二服務網路辨識符。該方法亦包括：使用該HSS的私密金鑰來解密來自由該UE加密的該資訊的、該第二服務網路辨識符和該KEK；及將該第一服務網路辨識符與該第二服務網路辨識符進行比較。當該第一服務網路辨識符與該第二服務網路辨識符匹配時，該方法包括：使用該服務網路的該節點的該公開金鑰來加密該KEK，以獲取加密的KEK；使用該KEK來加密該認證向量，以獲取加密的認證向量；及發送對該認證資訊請求的回應，其中該回應包括該加密的KEK和該加密的認證向量。

【0010】根據某些態樣，一種裝置包括：用於在UE和服務網路之間建立連接的單元；用於向與該UE相關聯的歸屬網路中的HSS傳輸第一訊息的單元，其中該第一訊息包括由該UE使用該HSS的加密金鑰來加密的認證憑證；及用於基於比較來認證該網路節點的單元，該比較是由該服務網路提供的、該服務網路的第一標識與在該認證憑證中提供的、該服務網路的第二標識的比較。該HSS可以被配置為解密該認證憑證以獲取該第二標識和由該UE提供的KEK，並且被配置為向該服務網路的網路節點提供使用該網路節點的公開金鑰來加密的、該KEK的版本。該用於認證該網路節點的該單元可以被配置為在該網路節點已向該UE發送了使用該KEK簽名的認證請求之

後，認證該網路節點。

【圖式簡單說明】

【0011】 圖1是圖示網路架構的實例的示圖。

【0012】 圖2是圖示存取網路的實例的示圖。

【0013】 圖3是圖示針對使用者平面和控制平面的無線電協定架構的實例的示圖。

【0014】 圖4是圖示存取網路中的進化型節點B和使用者設備的實例的示圖。

【0015】 圖5圖示可能在LTE網路內實現的E-UTRAN金鑰層的實例。

【0016】 圖6圖示可能在LTE封包交換網路中操作的通訊設備中實現的協定堆疊的實例。

【0017】 圖7是圖示LTE無線網路中的認證的實例的訊息流程圖。

【0018】 圖8是圖示LTE無線網路中的漏洞 (vulnerability) 的實例的示圖。

【0019】 圖9是圖示LTE無線網路中的假冒 (impersonation) 的實例的示圖。

【0020】 圖10是圖示根據本文揭示的某些態樣的認證程序的實例的訊息流程圖。

【0021】 圖11是圖示一種裝置的實例的方塊圖，該裝置採用可能根據本文揭示的某些態樣被適配的處理電路。

【0022】 圖12是根據本文揭示的某些態樣在UE處執行的無線通訊的方法的流程圖。

【0023】圖13圖示針對一種裝置的硬體實現的第一實例，該裝置例如根據本文揭示的一或多個態樣適配的UE。

【0024】圖14是根據本文揭示的某些態樣在MME處執行的無線通訊的方法的流程圖。

【0025】圖15圖示針對根據本文所揭示的一或多個態樣適配的MME裝置的硬體實現的第一實例。

【0026】圖16是根據本文揭示的某些態樣在HSS處執行的無線通訊的方法的流程圖。

【0027】圖17圖示針對根據本文所揭示的一或多個態樣適配的一種HSS裝置的硬體實現的實例。

【實施方式】

【0028】在下面結合附圖所闡述的詳細描述，意欲作為對各種配置的描述，而不意欲表示本文中所描述的概念可以以其實踐的唯一配置。出於提供給對各種概念的透徹理解的目的，詳細描述包括特定的細節。但是，對於本發明所屬領域中具有通常知識者來說將顯而易見的是，可以在不具有這些特定細節的情況下實踐這些概念。在一些實例中，為了避免模糊這些概念，以方塊圖形式示出公知的結構和元件。

【0029】現將參照各種裝置和方法來呈現電信系統的若干態樣。這些裝置和方法在下面的詳細描述中進行描述，並且在附圖中經由各種方塊、模組、元件、電路、步驟、程序、演算法等等（其統稱為「要素」）來示出。可以使用電子硬體、電腦軟體或者其任意組合來實現這些要素。至於這些要素是實現成硬體還是實現成軟體，取決於具體的應用和對整個

系統所施加的設計約束條件。

【0030】經由實例的方式，要素、或者要素的任意部分、或者要素的任意組合，可以用包括一或多個處理器的「處理系統」來實現。處理器的實例係包括微處理器、微控制器、數位訊號處理器（DSP）、現場可程式設計閘陣列（FPGA）、可程式設計邏輯裝置（PLD）、狀態機、閘控邏輯裝置、個別硬體電路和被配置為執行貫穿本案內容所描述的各種功能的其他適當硬體。處理系統中的一或多個處理器可以執行軟體。無論被稱為軟體、韌體、中介軟體、微代碼、硬體描述語言還是其他術語，軟體應當被廣意地解釋為意味著指令、指令集、代碼、程式碼片段、程式碼、程式、副程式、軟體模組、應用、軟體應用、套裝軟體、常式、子常式、物件、可執行檔、執行的執行緒、程序、函數等等。

【0031】因此，在一或多個示例性的設計方案中，所描述的功能可以在硬體、軟體、韌體或其任意組合中實現。若在軟體中實現，則可以將這些功能儲存或編碼為電腦可讀取儲存媒體上的一或多個指令或代碼。電腦可讀取媒體包括電腦儲存媒體。電腦可讀取媒體可以包括可以由一或多個處理器讀取及/或操縱的臨時性儲存媒體和非臨時性儲存媒體。儲存媒體可以是電腦能夠存取的任何可用媒體。經由實例的方式而不是限制的方式，這種電腦可讀取媒體可以包括隨機存取記憶體（RAM）、唯讀記憶體（ROM）、可程式設計ROM（PROM）、可抹除PROM（EPROM）、電子可抹除PROM（EEPROM）、壓縮光碟唯讀記憶體（CD-ROM）或其他光碟記憶體、磁

碟記憶體或其他磁存放裝置、或者能夠用於攜帶或儲存具有指令或資料結構形式的期望的程式碼並能夠由電腦存取的任何其他媒體。如本文中所使用的，磁碟和光碟包括壓縮光碟（CD）、鐳射光碟、光碟、數位多功能光碟（DVD）和軟碟，其中磁碟通常磁性地複製資料，而光碟則用鐳射來光學地複製資料。上面的組合亦應當包括在電腦可讀取媒體的保護範疇之內。

【0032】本文所揭示的某些態樣涉及經由其可以保護無線鏈路建立及/或承載建立程序的安全的系統和方法。本案內容的某些態樣解決了在新一代的無線存取技術（RAT）（包括第五代（5G）和以後的網路，以及第四代（4G）和更早的網路）中可能出現的安全問題。在本文中經由實例的方式來描述4G LTE網路架構的配置和操作，並且出於簡化某些態樣的描述的目的，其可適用於多種RAT。

【0033】圖1是圖示LTE網路架構100的示圖。LTE網路架構100可以稱為進化的封包系統（EPS）。EPS 100可以包括一或多個使用者設備（UE）102、進化的UMTS陸地無線電存取網路（E-UTRAN）104、進化的封包核心（EPC）110、歸屬用戶伺服器（HSS）120、和服務供應商的IP服務122。EPS可以與其他存取網路互連，但為了簡單起見，未圖示這些實體/介面。如圖所示，EPS提供封包交換服務，然而，如本發明所屬領域中具有通常知識者將容易理解的，貫穿本案內容提供的各種概念可以擴展到提供電路交換服務的網路。

【0034】E-UTRAN包括進化型節點B（eNodeB）106和其他

eNodeB 108。eNodeB 106提供了朝向UE 102的使用者和控制平面協定終止。eNodeB 106可以經由回載（例如，X2介面）連接到其他eNodeB 108。eNodeB 106亦可以被稱為基地台、基地台收發台、無線電基地台、無線電收發機、收發機功能單元、基本服務集（BSS）、擴展服務集（ESS）、eNB、或一些其他的適當術語。eNodeB 106為UE 102提供了到EPC 110的存取點。UE 102的實例係包括蜂巢式電話、智慧型電話、對話啟動協定（SIP）電話、膝上型電腦、個人數位助理（PDA）、衛星無線電設備、全球定位系統、多媒體設備、視訊設備、數位音訊播放機、（例如MP3播放機）、照相機、遊戲控制台、虛擬實境設備、平板計算設備、媒體播放機、電器、遊戲裝置、如智慧手錶或光學頭戴式顯示器的可穿戴計算設備、或任何其他類似功能的設備。UE 102亦可以被本發明所屬領域中具有通常知識者稱為行動站、用戶站、行動單元、用戶單元、無線單元、遠端單元、行動設備、無線設備、無線通訊設備、遠端設備、行動用戶站、存取終端、行動終端、無線終端、遠端終端機、手持設備、使用者代理、行動客戶端、客戶端、或者一些其他的適當術語。

【0035】 eNodeB 106由「S1」介面連接到EPC 110。EPC 110包括行動性管理實體（MME）112、其他MME 114、服務閘道116、和封包資料網路（PDN）閘道118。MME 112是處理UE 102和EPC 110之間的信號傳送的控制節點。通常，MME 112提供承載和連接管理。所有的使用者IP封包皆是經由服務閘道116進行傳送的，服務閘道116本身連接到PDN閘道118。PDN閘道

118提供UE IP位址分配以及其他功能。PDN閘道118連接到服務供應商的IP服務122。服務供應商的IP服務122可以包括網際網路、網內網路、IP多媒體子系統（IMS）以及PS流服務（PSS）。

【0036】圖2是圖示LTE網路架構中的存取網路200的實例的示圖。在這個實例中，將存取網路200劃分成數個蜂巢區域（細胞）202。一或多個較低功率級的eNodeB 208可以具有與細胞202中的一或多個重疊的蜂巢區域210。較低功率級的eNodeB 208可以是毫微微細胞（例如家庭eNodeB（HeNodeB））、微微細胞、微細胞或遠程無線電頭端（RRH）。每個宏eNodeB 204被分配給相應的細胞202並且經配置為細胞202中的所有UE 206提供到EPC 110的存取點。在存取網路200的這個實例中沒有集中式控制器，但是可以在可替代的配置中使用集中式控制器。eNodeB 204負責所有無線電相關的功能，包括無線電承載控制、許可控制、行動性控制、排程、安全性、以及到服務閘道116的連線性。

【0037】由存取網路200採用的調制和多工存取方案可以取決於所布署的具體電信標準而變化。在LTE應用中，OFDM用在DL上並且SC-FDMA用在UL上以支援分頻雙工（FDD）和分時雙工（TDD）二者。如本發明所屬領域中具有通常知識者根據接下來的詳細描述將容易理解的，本文中提供的各種概念良好地適用於LTE應用。然而，這些概念可以容易地擴展到採用其他調制和多工存取技術的其他電信標準。經由實例的方式，這些概念可以擴展到進化資料最佳化（EV-DO）或超

行動寬頻（UMB）。EV-DO和UMB是由第三代合作夥伴計畫2（3GPP2）公佈的、作為CDMA2000標準族一部分的空中介面標準並且採用CDMA以提供到行動站的寬頻網際網路存取。這些概念亦可以擴展到採用寬頻CDMA（W-CDMA）和CDMA的其他變型的通用陸地無線存取（UTRA），例如TD-SCDMA；採用TDMA的行動通訊全球系統（GSM）；和採用OFDMA的進化的UTRA（E-UTRA）、IEEE 802.11（Wi-Fi）、IEEE 802.16（WiMAX）、IEEE 802.20和Flash-OFDM。在來自3GPP組織的文件中描述了UTRA、E-UTRA、UMTS、LTE和GSM。在來自3GPP2組織的文件中描述了CDMA2000和UMB。實際所採用的無線通訊標準和多工存取技術將取決於具體應用和對系統施加的整體設計約束。

【0038】 eNodeB 204可以具有支援MIMO技術的多個天線。MIMO技術的使用使得eNodeB 204能夠利用空間域來支援空間多工、波束成形和發射分集。空間多工可以用於在同一個頻率上同時發送不同的資料串流。可以將資料串流發送給單個UE 206以提高資料速率或發送給多個UE 206以提高整體系統容量。這可以經由對每個資料串流進行空間預編碼（即施加振幅和相位的縮放）並且隨後經由DL上的多個發送天線來發送每個空間預編碼的流來實現。到達UE（206）處的空間預編碼的資料串流具有不同的空間簽名，這使得每個UE 206能夠恢復去往UE 206的一或多個資料串流。在UL上，每個UE 206發送空間預編碼的資料串流，這使得eNodeB 204能夠辨識每個空間預編碼的資料串流的源。

【0039】當通道狀況良好時，通常使用空間多工。當通道狀況較差時，可以使用波束成形來將傳輸能量集中到一或多個方向上。這可以由對經由多個天線進行發送的資料進行空間預編碼來實現。爲了在細胞的邊緣獲得良好的覆蓋，可以結合發射分集來使用單個流波束成形傳輸。

【0040】在接下來的詳細描述中，將參照在DL上支援OFDM的MIMO系統來描述存取網路的各個態樣。OFDM是在OFDM符號內的數個次載波上調制資料的展頻技術。次載波以精確的頻率間隔開。該間隔提供了使得接收器能夠從次載波恢復資料的「正交性」。在時域中，可以向每個OFDM符號添加保護間隔（例如循環字首）以對抗OFDM符號間干擾。UL可以使用DFT擴展OFDM信號的形式的SC-FDMA以補償高的峰均功率比（PAPR）。

【0041】圖3是圖示LTE中針對使用者平面和控制平面的無線協定架構的實例的示圖300。針對UE和eNodeB的無線電協定架構被示出爲具有三層：層1、層2和層3。層1（L1層）是最低層並且實現各種實體層信號處理功能。L1層在本文中將被稱爲實體層306。層2（L2層）308在實體層306之上並且負責實體層306上的、UE和eNodeB之間的鏈路。

【0042】在使用者平面中，L2層308包括媒體存取控制（MAC）子層310、無線電鏈路控制（RLC）子層312和封包資料彙聚協定（PDCP）子層314，這些子層終止於網路側的eNodeB處。儘管未圖示，但UE可以具有在L2層308之上的若干上層，該等若干上層包括終止於網路側的PDN閘道118處的網路層（例

如，IP層），以及終止於連接的另一端（例如遠端UE、伺服器）處的應用層。

【0043】 PDCP子層314提供不同的無線電承載和邏輯通道之間的多工。PDCP子層314亦提供針對上層資料封包的標頭壓縮以減少無線電傳輸管理負擔，經由加密資料封包提供安全性，並且針對UE提供eNodeB之間的切換支援。RLC子層312提供上層資料封包的分段和重組、丟失資料封包的重傳以及資料封包的重新排序以補償由混合自動重傳請求（HARQ）導致的無序接收。MAC子層310提供邏輯通道和傳輸通道之間的多工。MAC子層310亦負責在UE之間分配一個細胞中的各種無線電資源（例如，資源區塊）。MAC子層310亦負責HARQ操作。

【0044】 在控制平面中，除了以下的例外之處，針對UE和eNodeB的無線電協定架構對於實體層306和L2層308是基本相同的，該例外之處是：對於控制平面而言沒有標頭壓縮功能。控制平面亦包括層3（L3層）中的無線電資源控制（RRC）子層316。RRC子層316負責獲取無線電資源（即無線電承載）並且負責使用eNodeB和UE之間的RRC訊號傳遞來配置較低層。

【0045】 圖4是在存取網路中與UE 450通訊的eNodeB 410的方塊圖。在DL中，向控制器/處理器475提供來自核心網路的上層封包。控制器/處理器475實現L2層的功能性。在DL中，控制器/處理器475提供標頭壓縮、加密、封包分段和重新排序、邏輯通道和傳輸通道之間的多工，以及基於各種優先順序

度量的到UE 450的無線電資源配置。控制器/處理器475亦負責HARQ操作、對丟失封包的重發、以及到UE 450的訊號傳遞。

【0046】發射（TX）處理器416實現針對L1層（即實體層）的各種信號處理功能。信號處理功能包括：編碼和交錯以促進UE 450處的前向糾錯（FEC），和基於各種調制方案（例如二進位移相鍵控（BPSK）、正交移相鍵控（QPSK）、M移相鍵控（M-PSK）、M正交幅度調制（M-QAM））向信號群集進行映射。隨後將經編碼和經調制的符號分離成並行串流。隨後將每個串流映射到OFDM次載波、在時域及/或頻域上與參考信號（例如引導頻）進行多工處理、並且隨後使用反向快速傅裡葉變換（IFFT）組合在一起以產生攜帶時域OFDM符號串流的實體通道。對OFDM串流進行空間預編碼以產生多個空間串流。可以使用來自通道估計器474的通道估計來決定編碼和調制方案，以及使用其用於空間處理。通道估計可以從參考信號及/或由UE 450發送的通道狀況回饋推導出。隨後經由分別的發射器418 TX將每個空間串流提供給不同的天線420。每個發射器418 TX將RF載波調制有相應的空間串流以用於傳輸。

【0047】在UE 450處，每個接收器454RX經由其相應的天線452接收信號。每個接收器454RX恢復調制到RF載波上的資訊並且向接收器（RX）處理器456提供資訊。RX處理器456實現L1層的各種信號處理功能。RX處理器456執行對資訊的空間處理以恢復去往UE 450的任何空間串流。若多個空間串流要

去往UE 450，則RX處理器456可以將它們組合成單個OFDM符號串流。隨後RX處理器456使用快速傅裡葉變換（FFT）將OFDM符號串流從時域轉換到頻域。頻域信號包括針對OFDM信號的每個次載波的分開的OFDM符號串流。經由決定由eNodeB 410發送的最可能的信號群集點來恢復和解調每個次載波上的符號和參考信號。這些軟決定可以基於由通道估計器458所計算的通道估計。隨後對軟決定進行解碼和解交錯以恢復最初由eNodeB 410在實體通道上發送的資料和控制信號。隨後將資料和控制信號提供給控制器/處理器459。

【0048】 控制器/處理器459實現L2層。控制器/處理器可以與儲存有程式碼和資料的記憶體460相關聯。記憶體460可以稱為電腦可讀取媒體。在UL中，控制器/處理器459提供了傳輸通道和邏輯通道之間的解多工、封包重組、解密、標頭解壓縮、控制信號處理以恢復來自核心網路的上層封包。隨後向資料槽462提供上層封包，該等上層封包表示L2層之上的所有協定層。亦可以向資料槽462提供各種控制信號用於L3處理。控制器/處理器459亦負責使用確認（ACK）及/或否定確認（NACK）協定進行檢錯以支援HARQ操作。

【0049】 在UL上，使用資料來源467來向控制器/處理器459提供上層封包。資料來源467表示L2層之上的所有協定層。類似於結合由eNodeB 410進行的DL傳輸來描述的功能性，控制器/處理器459基於eNodeB 410進行的無線電資源配置，經由提供標頭壓縮、加密、封包分段和重新排序、以及邏輯通道和傳輸通道之間的多工來實現針對使用者平面和控制平面的L2

層。控制器/處理器459亦負責HARQ操作、丟失封包的重發、和到eNodeB 410的信號傳送。

【0050】 TX處理器468可以使用由通道估計器458從參考信號或由eNodeB 410發送的回饋推導出的通道估計來選擇合適的編碼和調制方案，以及促進空間處理。可以經由分別的發射器454TX向不同的天線452提供由TX處理器468產生的空間串流。每個發射器454TX將RF載波調制有相應的空間串流以用於傳輸。

【0051】 以類似於結合UE 450處的接收器功能所描述的方式在eNodeB 410處對UL傳輸進行處理。每個接收器418RX經由其相應的天線420接收信號。每個接收器418RX恢復調制到RF載波上的資訊並且向RX處理器470提供資訊。RX處理器470可以實現L1層。

【0052】 控制器/處理器475實現L2層。控制器/處理器475可以與儲存有程式碼和資料的記憶體476相關聯。記憶體476可以被稱為電腦可讀取媒體。在UL中，控制器/處理器475提供傳輸通道和邏輯通道之間的解多工、封包重組、解密、標頭解壓縮、控制信號處理以恢復來自UE 450的上層封包。可以向核心網路提供來自控制器/處理器475的上層封包。控制器/處理器475亦負責使用ACK及/或NACK協定來檢錯，以支援HARQ操作。

LTE網路中的承載建立

【0053】 LTE網路中的無線電鏈路建立可以涉及向網路提供存取的存取點和通訊設備之間的一或多個無線電承載的建立

。無線電鏈路建立典型地包括安全性啓動交換。隨後可以經由無線電鏈路來建立通信期承載（其可能是邏輯承載或邏輯通道），並且可以經由通信期承載來建立一或多個服務及/或通訊。通信期承載、服務及/或通訊可以由一或多個安全金鑰來保護。

【0054】作為通信期承載建立的一部分，認證請求及/或一或多個金鑰交換可以發生。在根據LTE相容協定操作的網路中，金鑰可以由通訊設備基於由一或多個網路實體提供的演算法匯出。

E-UTRAN金鑰層的實例

【0055】圖5圖示典型的E-UTRAN金鑰層500，其可以在典型的LTE網路中實現。在通訊設備中，網路側的網路實體中的通用用戶標識模組（USIM）和認證中心（AuC）使用主金鑰（K）502來產生密碼金鑰（CK）504和完整性金鑰（IK）506。密碼金鑰（CK）504和完整性金鑰（IK）506隨後可以由網路實體中的通訊設備和歸屬用戶伺服器（HSS）使用，以產生存取安全管理實體金鑰（ K_{ASME} ）508。在LTE網路中操作的通訊設備的安全性啓動可以經由認證和金鑰協商程序（AKA）、非存取層（NAS）安全模式配置（NAS SMC）和存取層（AS）安全模式配置（AS SMC）來完成。AKA用於匯出 K_{ASME} 508，該 K_{ASME} 508隨後用作計算NAS金鑰510和512以及AS金鑰514、516、518和520的基礎金鑰。網路側的通訊設備和MME隨後可以使用 K_{ASME} 508來產生這些安全金鑰中的一或多個。

【0056】LTE封包交換網路可以以多個分層協定層來構造，

其中較低的協定層向上層提供服務並且每一層負責不同的任務。例如，圖6圖示協定堆疊600的實例，其可以在LTE封包交換網路中操作的通訊設備中實現。在這個實例中，LTE協定堆疊600包括實體（PHY）層604、媒體存取控制（MAC）層606、無線電鏈路控制（RLC）層608、封包資料彙聚協定（PDCP）層611、RRC層612、NAS層614和應用（APP）層616。NAS層614之下的層通常被稱為存取層（AS）層602。

【0057】 RLC層608可以包括一或多個通道610。RRC層612可以實現針對UE的各種監測模式（包括連接狀態和閒置狀態）。NAS層614可以維持該通訊設備的行動性管理上下文、封包資料上下文及/或其IP位址。要注意的是，其他層可能存在於該協定堆疊600中（例如，上方、下方、及/或示出的層之間），但出於說明的目的而將其省略。無線電/通信期承載613可以例如在RRC層612及/或NAS層614處建立。因此，通訊設備和MME可以使用NAS層614以產生安全金鑰 $K_{NAS\ enc}$ 510和 $K_{NAS-int}$ 512。類似地，通訊設備和eNodeB可以使用RRC層612以產生安全金鑰 K_{UP-enc} 516、 $K_{RRC-enc}$ 518和 $K_{RRC-int}$ 520。儘管安全金鑰 K_{UP-enc} 516、 $K_{RRC-enc}$ 518和 $K_{RRC-int}$ 520可以在RRC層612處產生，但是這些金鑰可以由PDCP層611使用，以保護訊號傳遞及/或使用使用者/資料通訊的安全。例如，金鑰 K_{UP-enc} 516可以由PDCP層611使用，以確保使用者/資料平面（UP）通訊的安全，而金鑰 $K_{RRC-enc}$ 518和 $K_{RRC-int}$ 520可以被用於保護PDCP層611處的訊號傳遞（亦即，控制）通訊的安全。

【0058】 在一個實例中，在建立這些安全金鑰（金鑰 $K_{NAS\ enc}$

510、 $K_{NAS-int}$ 512、 K_{UP-enc} 516、 $K_{RRC-enc}$ 518及/或 $K_{RRC-int}$ 520)之前，可以經由不安全的共用控制通道(CCCH)來發送去往/來自通訊設備的通訊(未受保護的或未加密的)。在建立了這些安全金鑰之後，可以經由專用控制通道(DCCH)來發送這些相同的使用者資料及/或控制/訊號傳遞通訊。

【0059】在LTE相容網路中的連接建立/通信期承載建立程序期間，若存在已經來自先前建立的通信期的、現有的本端NAS安全上下文，則AKA和NAS SMC程序是可選的。可以在服務請求、附著請求和追蹤區域更新(TAU)請求的時間重用(reuse)現有的NAS上下文。TAU請求可以由UE定期發送或當UE進入不與該UE相關聯的追蹤區域時發送，其中追蹤區域(或路由區域)可以是在其中UE能夠在無需首先更新網路的情況下進行移動的區域。

【0060】在AS(使用者平面和RRC)和NAS二者處皆可以使用被提供作為輸入之一的單個演算法標識來匯出用於加密和完整性演算法的安全金鑰。在NAS層(例如，NAS層614)處，其由存取節點(eNodeB)在NAS SMC程序期間在NAS安全模式命令中提供給通訊設備。在AS水平，要使用的演算法由無線電資源控制(RRC)安全模式命令提供。金鑰產生可以由金鑰推導函數(KDF)來完成，該函數例如HMAC-SHA-256函數。在產生NAS安全金鑰 $K_{NAS-enc}$ 510和完整性金鑰 $K_{NAS-int}$ 512以及RRC安全金鑰 K_{UP-enc} 516、 $K_{RRC-enc}$ 518和完整性金鑰 $K_{RRC-int}$ 520時，金鑰匯出函數KDF取若干類型的輸入，該等輸入包括安全性啟動交換期間由網路所提供的輸入演算法標識

。例如，該輸入演算法標識可以標識高級加密標準（AES）或「SNOW-3G」。

【0061】應當指出的是，在一些實現中，所有的安全金鑰（例如，NAS加密和完整性金鑰以及RRC加密和完整性金鑰）是使用相同的金鑰推導函數（KDF）來產生的，該等金鑰推導函數例如HMAC-SHA-256，其使用根/基礎金鑰（例如， K_{ASME} ）、一或多個固定的輸入、和複數個可能的輸入演算法標識中的一個（亦即，安全性金鑰=KDF（根/基礎金鑰、固定的輸入、演算法標識））。

AKA程序的實例

【0062】圖7是訊息流程圖700，其圖示LTE無線網路中的認證的實例。UE 702可以經由服務網路704連接到網路，以便獲取由網路服務供應商提供的來自歸屬網路706的服務。在承載建立期間，UE 702可以建立與歸屬網路706的HSS 712的連接。UE 702可以信任該HSS 712，而服務網路704的eNodeB 708可能是不被信任的。UE 702可以發送具有標識資訊（例如國際行動用戶標識（IMSI））的NAS附著請求720。MME 710接收該NAS附著請求720，並在認證資訊請求訊息722中向HSS 712轉發該請求720。認證資訊請求訊息722可以包括該UE 702的IMSI和服務網路辨識符（SN_id）。HSS 712可以利用認證資訊回應訊息724進行回應，該認證資訊回應訊息724包括認證值（AUTN）、預期結果值（XRES）亂數和 K_{ASME} 。AUTN與RAND是一起由AuC產生的，其向UE 702認證HSS 712。MME 710和HSS 712之間的訊息722、724在鏈路740和受保護的認證

、授權和計費協定（Diameter）上傳輸。

【0063】 MME 710向UE 702發送NAS認證請求726，UE 702用NAS認證回應訊息728進行回應。NAS認證請求726包括AUTN、RAND和金鑰集辨識符（ KSI_{ASME} ）。MME 710可以向UE 702發送非存取層（NAS）安全模式配置（NAS SMC）訊息730。UE 702隨後向MME 710發送「NAS安全模式完成」訊息732，MME 710向eNodeB 708用信號形式發送「S1AP初始上下文建立」訊息734。eNodeB 708隨後可以向UE 702發送RRC非存取層（NAS）安全模式配置（RRC SMC）訊息736，其用RRC安全模式完成訊息738進行回應（當準備好時）。

【0064】 在某些網路實施方式中，服務網路704在認證完成之後的一段時間是可信任的。在一個實例中，在認證之後，直到HSS 712執行另一個認證程序（AKA），服務網路704可以是可信任的。所建立的信任存活的持續時間可以由網路服務供應商決定。網路服務供應商可以配置信任的時段持續數個小時、數天或數個星期。

進化的網路技術中的安全性考慮的實例

【0065】 由於4G、5G和其他網路技術的發展，某些網路功能可能朝向網路的邊緣而被推動。例如，與MME相關聯的網路功能可以被分配具有小型細胞中的eNodeB的網路功能。在一些例子中，一或多個網路功能的重定位可以降低蜂巢核心網路上的信任或使其無效。

【0066】 在一個實例中，可以布署毫微微細胞或家庭eNodeB（HeNB），以經由寬頻連線來提供當地語系化的無線服務。

毫微微細胞可以被表徵為小的、低功率的蜂巢基地台，其典型地被設計為在家庭或小型商業環境中使用。毫微微細胞可以是任意小型細胞，其典型地具有有限範圍及/或有限數量的活動的附著UE，該等附著UE經由廣域網或連接來連接到網路服務供應商的網路。毫微微細胞可以在一或多個網路中可操作，該一或多個網路包括 WCDMA、GSM、CDMA2000、TD-SCDMA、WiMAX和LTE網路。較新的技術的布署及/或毫微微細胞的使用可能導致對在較少受到保護的及/或更容易受到攻擊的、分離的位置處的網路功能單元進行處理。出於這些和其他原因，由小型細胞或中繼節點提供的安全水平相對於由巨集細胞提供的安全性可能顯著降低。可能會期望對小型細胞的增加的布署和用於支援網路中的多跳的中繼器。

【0067】在另一個實例中，在某些較新的技術中的網路功能單元可能位於共用的系統，及/或在雲端環境中提供。在此類系統和環境中，網路和計算功能可以是虛擬化的，並且通常由協力廠商提供商管理。儘管網路服務供應商可能能夠保護至雲端的存取路徑的安全，但雲端內部的安全不能得到保證。在一些情況下，在虛擬（雲端）環境的內部安全和虛擬化系統效能之間做出折衷。在一些情況下，網路服務供應商不需要擁有用於連接UE的網路設備，及/或網路中的網路設備的不同元件可以由不同的服務供應商所擁有。服務供應商之間的減少的隔離可能會導致，並且一些網路服務供應商可能更容易獲取其他網路服務供應商的憑證。例如，當兩個網路服務供應商共用共同的eNodeB或MME時，第一網路服務供應商

的憑證可能更容易地由第二網路服務供應商挪用。

【0068】 當某些安全假設是無效的時，網路可能被暗示為是不安全的。例如在4G AKA中，該HSS是可信任的網路實體，而HSS可能是信任的根源（root）。UE和服務網路之間的相互認證可以依賴於HSS和服務網路之間的安全性。HSS代表UE來認證服務網路，並經由秘密頻道向服務網路提供針對UE的認證憑證。

【0069】 參考圖8，HSS 818和服務網路804之間的通訊通道（S6a參考點）816被假定為是安全的，並且在一些實例中，由認證、授權和計費協定來保護，該協定例如Diameter協定，其經由其傳輸層安全（TLS）協定提供加密（cryptographic）能力。在一些情況下，HSS 818和MME 810之間的通訊通道816可能是不夠安全的，並且在某些情況下，S6a參考點816是不受保護的。例如，當MME 810實體上位於不太安全的環境中（包括當MME 810與eNodeB 808共同位於公共空間中，或位於雲端計算或網路環境之內）時，安全問題可能會出現。由於在到MME 810的傳輸中針對UE 802的憑證（包括認證向量（AV）824）可能會被攻擊者820攔截，所以會發生威脅。在此類環境中，HSS 818和MME 810之間的安全連接並不一定意味著認證資訊請求是合法的。例如，安全連接可能由不執行針對上層協定的健全性檢查的代理伺服器來處理。

【0070】 圖9圖示一種場景，其中流氓（rogue）公用陸上行動網路（PLMN）906可能假冒由有效網路服務供應商提供的一或多個其他PLMN 908、910。如圖8所示，HSS 904和合法

的服務PLMN 908之間的通訊通道918、920的漏洞可能被利用，以使得流氓PLMN 906可以監測通訊通道918、920，以捕捉在HSS 904和有效的PLMN 910之間發送的IMSI和金鑰資訊922。在一些情況下，流氓PLMN 906中的MME可以假冒有效PLMN 910中的MME，以便基於捕捉的UE認證向量與UE 902建立通訊鏈路916。流氓PLMN 906中的網路實體隨後可以存取關於UE 902的資訊，並且可以監測源自UE 902的通訊。

改善的服務網路認證的實例

【0071】根據本文揭示的某些態樣，並繼續參考圖8，經由僅將HSS 818作為受信任的實體，可以避免假冒攻擊。UE 802可以提供給HSS 818能夠用於對憑證（亦即，AV）進行加密的金鑰。HSS 818可以使用所提供的金鑰來加密針對UE 802的憑證。HSS 818可以加密金鑰，使得僅期望的MME 810可以解密金鑰。期望的MME 810可以被辨識及/或經由網路操作來向HSS 818註冊。MME 810可以解密金鑰，並且隨後解密針對UE 802的憑證。因此，MME 810可以向UE 802證明對金鑰的知曉。以這種方式，UE 802可以直接地和明確地認證服務網路804，而無需依賴額外的安全協定，例如Diameter協定。

【0072】圖10是圖示無線網路中的認證的實例的訊息流程圖1000，其中UE 802直接地和明確地認證服務網路804。無線網路可以是LTE或5G網路或其一些衍生物。UE 802可以連接至服務網路804，以便從網路服務供應商提供的歸屬網路806獲取服務。在承載建立期間，UE 802可以與歸屬網路806的HSS 818建立安全的連接。UE 802可以信任HSS 818，而服務網路

804的eNodeB 808和MME 810可能是不被信任的。UE 802可以發送具有其IMSI和資訊的NAS附著請求1002，該資訊包括服務網路辨識符（SN_id）和隨機選擇的金鑰加密金鑰（KEK）。公共或共用的金鑰加密可以用於加密NAS附著請求1002中的資訊。若使用公開金鑰加密，則IMSI、SN_id和KEK可以使用HSS 818的公開金鑰進行加密。若使用共用金鑰加密，則SN_id和KEK可以使用UE 802和HSS 818之間共用的秘密金鑰來加密。由UE 802發送的SN_id反映UE 802所請求連接的服務網路的標識。

【0073】 MME 810接收NAS附著請求1002，並向HSS 818發送認證資訊請求1004。認證資訊請求1004可以包括NAS附著請求中提供的加密的資訊、MME 810所屬於的網路的SN_id和MME證書（其可能是MME 810的公開金鑰（PK_MME））。針對MME 810的證書的可以由網路服務供應商簽名。HSS 818可以解密來自於NAS附著請求1002中提供的加密的資訊的KEK和SN_id。HSS 818可以將之後解密的SN_id與由MME 810在認證資訊請求1004中發送的SN_id進行比較。若兩個SN_id匹配，則HSS 818準備並發送認證資訊回應1006。認證資訊回應1006可以包括KEK的加密的版本，其是使用MME 810的公開金鑰（PK_MME）加密的。認證資訊回應1006亦可以包括使用KEK加密的認證向量。

【0074】 MME 810接收認證資訊回應1006並使用其私密金鑰來解密認證資訊回應1006中的KEK。MME 810隨後可以使用KEK來解密認證資訊回應1006中的認證向量。MME 810隨後

可以向UE 802發送NAS認證請求1008，其中完整性由KEK來保護。認證請求1008包括認證參數（AUTN、RAND、eKSI），其中AUTN參數是認證符記，RAND參數是隨機或偽亂數，並且eKSI參數是由MME 810提供的進化的金鑰集辨識符。認證請求1008包括使用KEK經由訊息建立的簽名或訊息認證碼（MAC_KEK）。UE 802用NAS認證回應訊息1010進行回應。

【0075】MME 810可以向UE 802發送NAS安全模式命令（SMC）訊息1012，以在建立某些無線電承載之前啟動AS安全性。UE 802經由向MME 810發送「NAS安全模式完成」訊息1014進行回應，MME 810向eNodeB 808用信號形式發送「S1AP初始上下文建立」訊息1016。S1AP在E-UTRAN 104和進化的封包核心（EPC）110（見圖1）之間提供訊號傳遞服務。隨後eNodeB 808可以向UE 802發送RRC SMC訊息1018，UE 802用「RRC安全模式完成」訊息1020進行回應（當準備好時）。

【0076】圖11是圖示針對一種裝置的硬體實現的簡化實例的概念圖1100，該裝置採用可以被配置為執行本文揭示的一或多個功能的處理電路1102。根據本案內容的各個態樣，可以使用處理電路1102來實現如本文中揭示的要素、或要素的任意部分、或要素的任意組合。處理電路1102可以包括由硬體和軟體模組的某種組合控制的一或多個處理器1104。處理器1104的實例係包括微處理器、微控制器、數位訊號處理器（DSP）、現場可程式設計閘陣列（FPGA）、可程式設計邏輯裝置（PLD）、狀態機、定序器、閘控邏輯裝置、個別的硬體電路，和被配置為執行貫穿本案內容所描述的各種功能的其

他適當硬體。一或多個處理器1104可以包括執行特定功能並且可以由軟體模組1116中的一個來配置、增強或控制的專用處理器。一或多個處理器1104可以經由在初始化期間載入的軟體模組1116的組合來配置，並進一步經由在操作期間載入或卸載一或多個軟體模組1116來配置。

【0077】在圖示的實例中，處理電路1102可以使用匯流排架構來實現，該匯流排架構由匯流排1110來整體表示。取決於處理電路1102的特定應用和整體設計約束條件，匯流排1110可以包括任意數量的互連匯流排和橋接器。匯流排1110將各種電路連結在一起，該等各種電路包括一或多個處理器1104和記憶體1106。記憶體1106可以包括存放裝置和大量存放區設備，並且在本文中可以被稱為電腦可讀取媒體及/或處理器可讀取媒體。匯流排1110亦可以連結各種其他電路，例如定時源、計時器、周邊設備、電壓調節器和電源管理電路。匯流排介面1108可以在匯流排1110和一或多個收發機1112之間提供介面。可以針對由處理電路所支援的每個網路技術來提供收發機1112。在某些情況下，多種網路技術可以共用在收發機1112中發現的電路或處理模組中的一些或全部。每個收發機1112提供用於經由傳輸媒體與各種其他裝置進行通訊的單元。取決於裝置的性質，亦可以提供使用者介面1118（例如，小鍵盤、顯示器、揚聲器、麥克風、操縱桿），並且使用者介面1118可以直接地或經由匯流排介面1108通訊地耦合到匯流排1110。

【0078】處理器1104可以負責管理匯流排1110以及負責通用

處理，該通用處理可以包括執行儲存在電腦可讀取媒體（可以包括記憶體1106）中的軟體。在這態樣，處理電路1102（包括處理器1104）可以用於實現本文揭示的任意方法、功能和技術。記憶體1106可以用於儲存由處理器1104在執行軟體時所操縱的資料，並且該軟體可以被配置為實現本文中所揭示的任何一種方法。

【0079】處理電路1102中的一或多個處理器1104可以執行軟體。無論被稱為軟體、韌體、中介軟體、微代碼、硬體描述語言還是其他術語，軟體應當被廣意地解釋為意味著指令、指令集、代碼、程式碼片段、程式碼、程式、副程式、軟體模組、應用、軟體應用、套裝軟體、常式、子常式、物件、可執行檔、執行的執行緒、程序、函數、演算法等等。軟體可以以電腦可讀取的形式位於記憶體1106中或位於外部電腦可讀取媒體中。外部電腦可讀取媒體及/或記憶體1106可以包括非臨時性電腦可讀取媒體。經由舉例的方式，非臨時性電腦可讀取媒體包括：磁存放裝置（例如，硬碟、軟碟、磁條）、光碟（例如，壓縮光碟（CD）或數位多功能光碟（DVD））、智慧卡、快閃記憶體設備（例如，「快閃記憶體驅動器」、卡、棒、或鍵式磁碟）、隨機存取記憶體（RAM）、唯讀記憶體（ROM）、可程式設計ROM（PROM）、可抹除PROM（EPROM）、電子可抹除PROM（EEPROM）、暫存器、抽取式磁碟，以及用於儲存電腦能夠存取和讀取的軟體及/或指令的任何其他適當媒體。經由舉例的方式，電腦可讀取媒體及/或記憶體1106亦可以包括：載波、傳輸線、以及用於

傳輸電腦能夠存取和讀取的軟體及/或指令的任何其他適當媒體。電腦可讀取媒體及/或記憶體1106可以常駐在處理電路1102中、處理器1104中、處理電路1102外部，或跨越包括處理電路1102的多個實體而分佈。電腦可讀取媒體及/或記憶體1106可以體現在電腦程式產品中。經由舉例的方式，電腦程式產品可以包括封裝材料中的電腦可讀取媒體。本發明所屬領域中具有通常知識者將認識到如何取決於具體應用和施加於整個系統的整體設計約束來最好地實現貫穿本案內容呈現的所描述的功能。

【0080】記憶體1106可以維持以程式碼片段、模組、應用、程式等等維持及/或組織的軟體，其在本文中可以被稱為軟體模組1116。軟體模組1116中的每一個可以包括指令和資料，當其安裝或載入到處理電路1102上並由一或多個處理器1104執行時，促成執行時影像（run-time image）1114，其控制一或多個處理器1104的操作。當被執行時，某些指令可以使得處理電路1102執行根據本文所描述的某些方法、演算法和程序的功能。

【0081】軟體模組1116中的一些可以在處理電路1102的初始化期間被載入，並且這些軟體模組1116可以配置處理電路1102來啓用本文所揭示的各種功能的效能。例如，軟體模組1116中的一些可以配置內部設備及/或處理器1104的邏輯電路1122，並且可以管理對外部設備的存取，該等外部設備例如收發機1112、匯流排介面1108、使用者介面1118、計時器、數學輔助處理器等。軟體模組1116可以包括與中斷處理器和

裝置驅動程式互動、並且控制對由處理電路1102提供的各種資源的存取的控製程式及/或作業系統。資源可以包括記憶體、處理時間、對收發機1112的存取、使用者介面1118等等。

【0082】處理電路1102的一或多個處理器1104可以是多功能的，由此一些軟體模組1116被載入並且被配置為執行不同的功能或相同功能的不同實例。一或多個處理器1104可以額外適配為管理回應於來自例如使用者介面1118、收發機1112、和裝置驅動程式的輸入而發起的幕後工作。為了支援多種功能的效能，一或多個處理器1104可以被配置為提供多工環境，由此複數個功能之每一者功能被實現為一或多個處理器1104根據需要或期望而提供的任務集。在一個實例中，可以使用在不同任務之間傳遞處理器1104的 controls 的分時程式1120來實現多工環境，由此每個任務在完成了任何未完成的操作及/或回應於例如中斷的輸入時，向分時程式1120返回一或多個處理器1104的控制。當任務在一或多個處理器1104的控制下時，處理電路有效地專用於由與控制任務相關聯的功能處理的目的。分時程式1120可以包括作業系統、主循環、函數及/或中斷驅動主循環，該主循環在循環（round-robin）的基礎上傳遞控制，該函數根據功能的優先順序來分配一或多個處理器1104的控制，該中斷驅動主循環經由將一或多個處理器1104的控制提供給正在處理的功能來回應外部事件。

【0083】下面的流程圖圖示在根據本文中揭示的某些態樣適配或配置的網路元件上執行或可操作的方法和程序。該等方法和程序可以以任意適當的網路技術來實現，該網路技術包

括3G、4G、5G技術等等。因此，請求項並不受限於單個網路技術。在這點上，對「UE」的引用亦可以理解為指的是行動站、用戶站、行動單元、用戶單元、無線單元、遠端單元、行動設備、無線設備、無線通訊設備、遠端設備、行動用戶站、存取終端、行動終端、無線終端、遠端終端機、手持機、使用者代理、行動客戶端、客戶端、或一些其他適當的術語。對「eNodeB」的引用可以被理解為指的是基地台、基地台收發台、無線電基地台、無線電收發機、收發機功能單元、基本服務集、擴展服務集，或一些其他適當的術語。對MME的引用亦可以指的是例如作為服務網路中的認證器及/或諸如行動交換中心等主服務傳遞節點的實體。對HSS的引用亦可以指的是資料庫，其包含使用者相關和用戶相關資訊的資料庫、在行動性管理中提供支援功能、撥叫和通信期設置、及/或使用者認證和存取授權，其包括例如歸屬位置暫存器（HLR）、認證中心（AuC）及/或認證、授權和計費（AAA）伺服器。

【0084】圖12是無線通訊的方法的流程圖1200。該方法可以由UE執行。在方塊1202處，UE可以建立與服務網路的連接。

【0085】在方塊1204處，UE可以向服務網路的網路節點發送在第一訊息中的認證憑證，該認證憑證包括隨機選擇的KEK和服務網路辨識符。該網路節點可以是MME。認證憑證可以是使用與歸屬網路中的HSS的加密金鑰來加密的。在一些情況下，該認證憑證是基於與該HSS共用的金鑰，使用對稱密碼加密的。在一些情況下，認證憑證可以基於該HSS的公開金鑰，

使用非對稱密碼進行加密。

【0086】在方塊1206處，UE可以接收回應於該第一訊息的第二訊息。該第二訊息可以包括來自該網路節點的認證請求和由該網路節點使用該KEK產生的簽名。該第二訊息可以攜帶使用該KEK產生的訊息認證碼。該第二訊息可以由MME在該MME接收到對發送至HSS的認證資訊請求的回應之後產生。對該認證資訊請求的該回應可能是由該HSS發送至該MME的，並且是使用該MME的公開金鑰來加密的。

【0087】在方塊1208處，UE可以基於該簽名來認證該網路節點。

【0088】在一個實例中，當該簽名是使用該KEK的副本產生的時，該網路節點可以被認證。當在加密的訊息的交換期間，該網路節點已接收到該KEK的副本時，該簽名可能是使用該KEK的副本產生的，該加密的訊息的交換是與該HSS進行的、回應於該第一訊息由該網路節點發起的。

【0089】圖13是圖示針對採用處理電路1302的裝置1300的硬體實現的簡化實例的方塊示意圖。處理電路典型地具有處理器1316，該處理器1316可以包括微處理器、微控制器、數位訊號處理器、定序器和狀態機中的一或多個。處理電路1302可以使用匯流排架構來實現，該匯流排架構由匯流排1320來整體表示。取決於處理電路1302的特定應用和整體設計約束條件，匯流排1320可以包括任意數量的互連匯流排和橋接器。匯流排1320將各種電路連結在一起，該等各種電路包括一或多個處理器及/或硬體模組(由處理器1316、模組或電路1304

、1306和1308、無線收發機電路1312所表示)，無線收發機電路1312可配置為經由天線1314和電腦可讀取儲存媒體1318來進行通訊。匯流排1320亦可以連結各種其他電路，例如定時源、周邊設備、電壓調節器和電源管理電路，這在本發明所屬領域是公知的，並且因此將不再進一步描述。

【0090】處理器1316負責一般處理，包括執行電腦可讀取儲存媒體1318上儲存的軟體。當軟體由處理器1316執行時，使得處理系統1302執行以上針對任意具體裝置所描述的各種功能。該電腦可讀取儲存媒體1318亦可以用於儲存當處理器1316正在執行軟體時所操作的資料，該資料包括對從經由天線1314（其可以被配置為資料通道和時鐘通道）發送的符號解碼得到的資料。處理電路1302亦包括模組1304、1306和1308中的至少一個。模組1304、1306和1308可以是在處理器1316中執行、常駐/儲存在電腦可讀取儲存媒體1318中的軟體模組，耦合到處理器1316的一或多個硬體模組，或其一些組合。模組1304、1306及/或1308可以包括微控制器指令、狀態機配置參數，或其某些組合。

【0091】在一種配置中，用於無線通訊的裝置1300包括模組及/或電路1304、模組及/或電路1306以及模組及/或電路1308，模組及/或電路1304被配置為與歸屬網路建立連接，模組及/或電路1306被配置為處理用於與服務網路的通訊的加密和解密，模組及/或電路1308被配置為發送訊息以及接收訊息。在一個實例中，訊息在UE和服務網路之間傳輸。在另一個實例中，訊息在UE和歸屬網路之間傳輸。在另一個實例中，訊息

在服務網路和歸屬網路之間傳輸。

【0092】圖14是無線通訊的方法的流程圖1400。該方法可以由服務網路的實體（例如MME）來執行。在方塊1402處，MME可以接收來自UE的、用於建立與該服務網路的連接的第一請求。第一請求可以包括UE的唯一辨識碼和加密的資訊，該加密的資訊包括服務網路的辨識符和隨機選擇的KEK。

【0093】在方塊1404處，MME可以向與UE相關聯的歸屬網路的HSS發送第二請求。該請求可以包括在第一請求中接收到的加密的資訊和MME的公開金鑰。在該第一請求中接收到的該加密的資訊是由該UE使用該HSS的加密金鑰來加密的。

【0094】在方塊1406處，MME可以接收對來自HSS的對第二請求的回應。對該第二請求的該回應可以包括使用該MME的公開金鑰來加密的該KEK。對該第二請求的該回應可以包括使用該KEK加密的認證向量。

【0095】在方塊1408處，MME可以使用與MME的公開金鑰相對應的私密金鑰來解密該KEK。

【0096】在方塊1410處，MME可以使用該KEK來解密認證向量。

【0097】在方塊1412處，MME可以向UE發送第三請求。第三請求可以包括使用該KEK簽名的認證請求。

【0098】在一些情況下，MME可以接收到來自UE的對第三請求的回應，並且在接收到對該第三請求的該回應之後在UE與服務網路之間建立連接。

【0099】圖15是圖示針對採用處理電路1502的裝置1500的硬

體實現的簡化實例的示圖。處理電路典型地具有處理器1516，該處理器可以包括微處理器、微控制器、數位訊號處理器、定序器和狀態機中的一或多個。處理電路1502可以使用匯流排架構來實現，該匯流排架構由匯流排1520來整體表示。取決於處理電路1502的特定應用和整體設計約束條件，匯流排1520可以包括任意數量的互連匯流排和橋接器。匯流排1520將各種電路連結在一起，該等各種電路包括一或多個處理器及/或硬體模組（由處理器1516、模組或電路1504、1506、1508和1510、無線收發機電路1512所表示），無線收發機電路1512可配置為經由天線1514和電腦可讀取儲存媒體1518來進行通訊。匯流排1520亦可以連結各種其他電路，例如定時源、周邊設備、電壓調節器和電源管理電路，這在本發明所屬領域是公知的，因此將不再進一步描述。

【0100】處理器1516負責一般處理，包括執行電腦可讀取儲存媒體1518上儲存的軟體。當軟體由處理器1516執行時，使得處理系統1502執行以上針對任意具體裝置所描述的各種功能。該電腦可讀取儲存媒體1518亦可以用於儲存當處理器1516正在執行軟體時所操作的資料，該資料包括對從經由天線1514（其可以被配置為資料通道和時鐘通道）發送的符號解碼得到的資料。處理電路1502亦包括模組1504、1506和1508中的至少一個。模組1504、1506、1508和1510可以在處理器1516中執行、常駐/儲存在電腦可讀取儲存媒體1518中的軟體模組，耦合到處理器1516的一或多個硬體模組，或其一些組合。模組1504、1506、1508及/或1510可以包括微控制器指令

、狀態機配置參數，或其某些組合。

【0101】在一種配置中，用於無線通訊的裝置1500包括模組及/或電路1504、模組及/或電路1506以及模組及/或電路1508，模組及/或電路1504被配置為與一或多個UE建立連接，模組及/或電路1506被配置為管理或處理加密和解密程序，模組及/或電路1508被配置為向UE發送訊息以及從UE接收訊息及/或向HSS發送訊息以及從HSS接收訊息。

【0102】圖16是無線通訊的方法的流程圖1600。該方法可以由UE的歸屬網路中的HSS來執行。在方塊1602處，HSS可以接收來自服務網路的節點的認證資訊請求。服務網路的節點可以是MME。該請求可以包括第一服務網路辨識符、服務網路的節點的公開金鑰、以及由UE加密的資訊。由UE加密的資訊可以包括隨機選擇的KEK和第二服務網路辨識符。在一些情況下，由UE加密的資訊是基於與HSS共用的金鑰，使用對稱密碼加密的。在一些情況下，由UE加密的資訊是基於該HSS的公開金鑰，使用非對稱密碼加密的。

【0103】在方塊1604處，HSS可以使用HSS的私密金鑰來解密來自於由UE加密的資訊的、第二服務網路辨識符和該KEK。

【0104】在方塊1606處，HSS可以將第一服務網路辨識符與第二服務網路辨識符進行比較。

【0105】在方塊1608處，下一個方塊是基於該第一服務網路辨識符是否與第二服務網路辨識符匹配來決定的。當沒有找到匹配時，該方法可以在方塊1616處以認證失敗而終止。當發現匹配時，該方法可以在方塊1610處繼續。

【0106】在方塊1610處，HSS可以使用該服務網路的節點的公開金鑰來加密KEK，以獲取加密的KEK。

【0107】在方塊1612處，HSS可以使用該KEK來加密認證向量，以獲取加密的認證向量。

【0108】在方塊1614處，HSS可以發送對認證資訊請求的回應，其中該回應包括該加密的KEK和加密的認證向量。

【0109】圖17是圖示針對採用處理電路1702的裝置1700的硬體實現的簡化實例的示圖。處理電路典型地具有處理器1716，該處理器可以包括微處理器、微控制器、數位訊號處理器、定序器和狀態機中的一或多個。處理電路1702可以使用匯流排架構來實現，該匯流排架構由匯流排1720來整體表示。取決於處理電路1702的特定應用和整體設計約束條件，匯流排1720可以包括任意數量的互連匯流排和橋接器。匯流排1720將各種電路連結在一起，該等各種電路包括一或多個處理器及/或硬體模組（由處理器1716、模組或電路1704、1706和1708、無線收發機電路1712所表示），無線收發機電路1712可配置為經由天線1714和電腦可讀取儲存媒體1718來進行通訊。匯流排1720亦可以連結各種其他電路，例如定時源、周邊設備、電壓調節器和電源管理電路，這在本發明所屬領域是公知的，並且因此將不再進一步描述。

【0110】處理器1716負責一般處理，包括執行電腦可讀取儲存媒體1718上儲存的軟體。當軟體由處理器1716執行時，使得處理系統1702執行以上針對任意具體裝置所描述的各種功能。該電腦可讀取儲存媒體1718亦可以用於儲存當處理器

1716正在執行軟體時所操作的資料，該資料包括對從經由天線1714（其可以被配置為資料通道和時鐘通道）發送的符號解碼得到的資料。處理電路1702亦包括模組1704、1706和1708中的至少一個。模組1704、1706和1708可以是在處理器1716中執行、常駐/儲存在電腦可讀取儲存媒體1718中的軟體模組，耦合到處理器1716的一或多個硬體模組，或其一些組合。模組1704、1706及/或1708可以包括微控制器指令、狀態機配置參數，或其某些組合。

【0111】在一種配置中，用於無線通訊的裝置1700包括模組及/或電路1704、模組及/或電路1706以及模組及/或電路1708，模組及/或電路1704被配置為管理與歸屬網路相關聯的加密金鑰，模組及/或電路1706被配置為管理或執行與在歸屬網路內以及在歸屬網路與服務網路之間發送的訊息有關的加密和解密，模組及/或電路1708被配置為向服務網路發送訊息以及從服務網路接收訊息。

【0112】應當理解的是，所揭示的程序中步驟的特定順序或層次是對示例性方法的說明。應當理解的是，基於設計偏好，可以重新排列程序中步驟的特定順序或層次。此外，可以組合或者省略一些步驟。所附的方法請求項以取樣順序來呈現各種步驟的要素，但並不意味著其要受限於所呈現的特定順序或層次。

【0113】為使本發明所屬領域中具有通常知識者能夠實踐本文中所描述的各個態樣，提供了之前的描述。對於本發明所屬領域中具有通常知識者來說，對這些態樣的各種修改將是

顯而易見的，並且，本文中定義的一般原理可以適用於其他態樣。因此，請求項並不是要限於本文中所示出的態樣，而是要符合與請求項語言相一致的全部範疇，其中以單數形式來參考的要素並不意欲意味著「一個並且只有一個」（除非特別如此說明），而指的是「一或多個」。除非另外特別說明，否則術語「一些」指的是一或多個。貫穿本案內容來描述各個態樣的要素的所有結構均等物和功能均等物（對於本發明所屬領域中具有通常知識者來說是已知的或稍後要知道的）經由引用明確地併入本文，並且意欲由請求項所包含。另外，本文中揭示的所有內容均不是要貢獻給公眾的，不論這種揭示內容是否在請求項中進行了明確地陳述。請求項的任何要素皆不應當被解釋為功能單元，除非該要素使用短語「用於……的單元」來明確地陳述。

【符號說明】

【0114】

100 LTE 網路架構

102 使用者設備（UE）

104 進化的 UMTS 陸地無線電存取網路（E-UTRAN）

106 進化型節點 B（eNodeB）

108 其他 eNodeB

110 進化的封包核心（EPC）

112 行動性管理實體（MME）

114 其他 MME

116 服務閘道

- 118 封包資料網路 (PDN) 閘道
- 120 歸屬用戶伺服器 (HSS)
- 122 服務供應商的 IP 服務
- 200 存取網路
- 202 蜂巢區域 (細胞)
- 204 宏 eNodeB
- 206 UE
- 208 較低功率級的 eNodeB
- 210 蜂巢區域
- 300 示圖
- 306 實體層
- 308 L2 層
- 310 媒體存取控制 (MAC) 子層
- 312 無線電鏈路控制 (RLC) 子層
- 314 封包資料彙聚協定 (PDCP) 子層
- 316 無線電資源控制 (RRC) 子層
- 410 eNodeB
- 416 發射 (TX) 處理器
- 418 發射器
- 420 天線
- 450 UE
- 452 天線
- 454 接收器
- 456 接收器 (RX) 處理器

- 458 通道估計器
- 459 控制器/處理器
- 460 記憶體
- 462 資料槽
- 467 資料來源
- 468 TX 處理器
- 470 RX 處理器
- 474 通道估計器
- 475 控制器/處理器
- 476 記憶體
- 502 主金鑰 (K)
- 504 密碼金鑰 (CK)
- 506 完整性金鑰 (IK)
- 508 存取安全管理實體金鑰 (K_{ASME})
- 510 算 NAS 金鑰
- 512 算 NAS 金鑰
- 514 AS 金鑰
- 516 AS 金鑰
- 518 AS 金鑰
- 520 AS 金鑰
- 600 協定堆疊
- 602 存取層 (AS) 層
- 604 實體 (PHY) 層
- 606 媒體存取控制 (MAC) 層

- 608 無線電鏈路控制（RLC）層
- 610 通道
- 611 封包資料彙聚協定（PDCP）層
- 612 RRC 層
- 613 無線電/通信期承載
- 614 NAS 層
- 616 應用（APP）層
- 700 訊息流程圖
- 702 UE
- 704 服務網路
- 706 歸屬網路
- 708 eNodeB
- 710 MME
- 712 HSS
- 720 NAS 附著請求
- 722 NAS 附著請求
- 724 認證資訊回應訊息
- 726 NAS 認證請求
- 728 NAS 認證回應訊息
- 730 非存取層（NAS）安全模式配置（NAS SMC）訊息
- 732 「NAS 安全模式完成」訊息
- 734 「S1AP 初始上下文建立」訊息
- 736 RRC 非存取層（NAS）安全模式配置（RRC SMC）訊息
- 738 RRC 安全模式完成訊息

740 鏈路

802 UE

804 服務網路

806 歸屬網路

808 eNodeB

810 MME

816 S6a 參考點

818 HSS

820 攻擊者

824 認證向量 (AV)

902 UE

904 HSS

906 公用陸上行動網路 (PLMN)

908 PLMN

910 PLMN

916 通訊鏈路

918 通訊通道

920 通訊通道

1000 訊息流程圖

1002 NAS 附著請求

1004 認證資訊請求

1006 認證資訊回應

1008 NAS 認證請求

1010 NAS 認證回應訊息

- 1012 NAS 安全模式命令（SMC）訊息
- 1014 「NAS 安全模式完成」訊息
- 1016 「S1AP 初始上下文建立」訊息
- 1018 RRC SMC 訊息
- 1020 「RRC 安全模式完成」訊息
- 1100 概念圖
- 1102 處理電路
- 1104 處理器
- 1106 記憶體
- 1108 匯流排介面
- 1110 匯流排
- 1112 收發機
- 1114 執行時影像
- 1116 處理器
- 1118 使用者介面
- 1120 分時程式
- 1122 邏輯電路
- 1200 流程圖
- 1202 方塊
- 1204 方塊
- 1206 方塊
- 1208 方塊
- 1300 裝置
- 1302 處理電路

- 1304 模組或電路
- 1306 模組或電路
- 1308 模組或電路
- 1312 無線收發機電路
- 1314 天線
- 1316 處理器
- 1318 天線
- 1320 匯流排
- 1400 流程圖
- 1402 方塊
- 1404 方塊
- 1406 方塊
- 1408 方塊
- 1410 方塊
- 1412 方塊
- 1500 裝置
- 1502 處理電路
- 1504 模組或電路
- 1506 模組或電路
- 1508 模組或電路
- 1510 模組或電路
- 1512 無線收發機電路
- 1514 天線
- 1516 處理器

- 1518 電腦可讀取儲存媒體
- 1600 流程圖
- 1602 方塊
- 1604 方塊
- 1606 方塊
- 1608 方塊
- 1610 方塊
- 1612 方塊
- 1614 方塊
- 1616 方塊
- 1700 裝置
- 1702 處理電路
- 1704 模組或電路
- 1706 模組或電路
- 1708 模組或電路
- 1712 無線收發機電路
- 1714 天線
- 1716 處理器
- 1718 電腦可讀取儲存媒體
- 1720 匯流排

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

無

【序列表】(請換頁單獨記載)

無

申請專利範圍

1. 一種用於在一使用者設備（UE）處的無線通訊的方法，包括以下步驟：

由該UE建立與一服務網路的一連接；

由該UE向該服務網路發送包括一認證憑證的一第一訊息，該認證憑證包括一隨機選擇的金鑰加密金鑰（KEK）和一服務網路辨識符，其中該認證憑證是使用與一歸屬網路相關聯的一加密金鑰來加密的；

由該UE接收回應於該第一訊息的一第二訊息，其中該第二訊息包括來自該服務網路的一認證請求和由該服務網路的一節點使用該KEK產生的一簽名；及

由該UE基於該簽名來認證該服務網路。

2. 根據請求項1之方法，其中認證該服務網路包括以下步驟：

當該簽名是使用該KEK的一副本產生的時，認證該服務網路，其中當該服務網路在一加密的訊息的交換期間已接收到該KEK的一副本時，該簽名是使用該KEK的一副本產生的，該加密的訊息的交換是與該歸屬網路進行的、回應於該第一訊息由該服務網路的一節點發起的。

3. 根據請求項1之方法，其中該簽名是由該服務網路的一行動性管理實體（MME）產生的。

4. 根據請求項1之方法，其中該認證憑證是基於該UE和該歸屬網路的一節點之間共用的一金鑰，使用一對稱密碼加密的。
5. 根據請求項4之方法，其中該歸屬網路的該節點包括一歸屬用戶伺服器（HSS）。
6. 根據請求項4之方法，其中該歸屬網路的該節點包括一認證、授權、和計費（AAA）伺服器。
7. 根據請求項4之方法，其中該認證憑證是基於該歸屬網路的一節點的一公開金鑰，使用一不對稱的密碼加密的。
8. 根據請求項4之方法，其中該歸屬網路的該節點包括一歸屬用戶伺服器（HSS）。
9. 根據請求項4之方法，其中該歸屬網路的該節點包括一認證、授權、和計費（AAA）伺服器。
10. 根據請求項1之方法，其中該第二訊息包括使用該KEK產生的一訊息認證碼。
11. 根據請求項10之方法，其中該第二訊息是由一MME在該MME接收到對發送至一HSS的一認證資訊請求的一回應之後

產生的，其中對該認證資訊請求的該回應是由該HSS發送至該MME的，並且是使用該MME的一公開金鑰來加密的。

12. 一種用於一服務網路中的無線通訊的方法，包括以下步驟：

由該服務網路的一節點接收來自一使用者設備（UE）的一第一請求，該第一請求用於在該UE和該服務網路之間建立一連接，該第一請求包括該UE的一唯一辨識碼和加密的資訊，該加密的資訊包括該服務網路的一辨識符和一隨機選擇的金鑰加密金鑰（KEK）；

由該服務網路的該節點向與該UE相關聯的一歸屬網路發送一第二請求，該第二請求包括在該第一請求中接收到的該加密的資訊和該服務網路的該節點的一公開金鑰；

由該服務網路的該節點接收來自該歸屬網路的對該第二請求的一回應，對該第二請求的該回應包括使用該服務網路的該節點的一公開金鑰加密的該KEK，以及使用該KEK加密的一認證向量；

由該服務網路的該節點使用與該服務網路的該節點的該公開金鑰相對應的一私密金鑰來解密該KEK；

由該服務網路的該節點使用該KEK來解密該認證向量；
及

由該服務網路的該節點向該UE發送一第三請求，該第三請求包括使用該KEK簽名的一認證請求。

13. 根據請求項12之方法，其中在該第一請求中接收到的該加密的資訊是由該UE使用該歸屬網路的一加密金鑰來加密的。

14. 根據請求項12之方法，亦包括以下步驟：

接收來自該UE的對該第三請求的一回應；及

在接收到對該第三請求的該回應之後，在該UE和該服務網路之間建立一連接。

15. 一種用於一使用者設備（UE）的一歸屬網路中的無線通訊的方法，包括以下步驟：

由該歸屬網路的一節點接收來自一服務網路的一節點的一認證資訊請求，其中該請求包括一第一服務網路辨識符、該服務網路的該節點的一公開金鑰、以及由該UE加密的資訊，由該UE加密的該資訊包括一隨機選擇的金鑰加密金鑰（KEK）和一第二服務網路辨識符；

使用該歸屬網路的一私密金鑰來解密來自由該UE加密的該資訊的、該第二服務網路辨識符和該KEK；

將該第一服務網路辨識符與該第二服務網路辨識符進行比較；及

當該第一服務網路辨識符與該第二服務網路辨識符匹配時：

使用該服務網路的該節點的該公開金鑰來加密該KEK，以獲取一加密的KEK；

使用該KEK來加密一認證向量，以獲取一加密的認證向量；及

發送對該認證資訊請求的一回應，其中該回應包括該加密的KEK和該加密的認證向量。

16. 根據請求項15之方法，其中該服務網路的該節點包括一行動性管理實體（MME）。

17. 根據請求項15之方法，其中由該UE加密的該資訊是基於該UE和該歸屬網路的一節點之間共用的一金鑰，使用一對稱密碼加密的。

18. 根據請求項17之方法，其中該歸屬網路的該節點包括一歸屬用戶伺服器（HSS）。

19. 根據請求項17之方法，其中該歸屬網路的該節點包括一認證、授權、和計費（AAA）伺服器。

20. 根據請求項15之方法，其中由該UE加密的該資訊是基於該歸屬網路的一節點的一公開金鑰，使用一不對稱的密碼加密的。

21. 根據請求項20之方法，其中該歸屬網路的該節點包括一歸屬用戶伺服器（HSS）。

22. 根據請求項20之方法，其中該歸屬網路的該節點包括一認證、授權、和計費（AAA）伺服器。

23. 一種裝置，包括：

用於在一使用者設備（UE）和一服務網路之間建立一連接的單元；

用於向與該UE相關聯的一歸屬網路傳輸一第一訊息的單元，其中該第一訊息包括由該UE使用該歸屬網路的一加密金鑰來加密的一認證憑證；及

用於基於一比較來認證該服務網路的單元，該比較是由該服務網路的一節點提供的、該服務網路的一第一標識與在該認證憑證中提供的、該服務網路的一第二標識的比較，

其中該歸屬網路的該節點被配置為解密該認證憑證以獲取該第二標識和由該UE提供的一金鑰加密金鑰（KEK），並且被配置為向該服務網路的該節點提供使用該服務網路的該節點的一公開金鑰來加密的、該KEK的一版本，並且

其中用於認證該服務網路的該單元被配置為在該服務網路的該節點已向該UE發送了使用該KEK簽名的一認證請求之後，認證該服務網路。

24. 根據請求項23之裝置，其中該服務網路的該節點包括一行動性管理實體（MME）。

25. 根據請求項23之裝置，其中用於認證該服務網路的該單元被配置為：

當該網路使用由該歸屬網路的該節點提供的該KEK的該版本產生一簽名時，認證該服務網路的該節點。

26. 根據請求項23之裝置，其中該認證憑證是基於該UE和該歸屬網路的一節點之間共用的一金鑰，使用一對稱密碼加密的。

27. 根據請求項26之裝置，其中該歸屬網路的該節點包括一歸屬用戶伺服器（HSS）或認證、授權、和計費（AAA）伺服器。

28. 根據請求項23之裝置，其中該認證憑證是基於該歸屬網路的一節點的一公開金鑰，使用一不對稱的密碼加密的。

29. 根據請求項28之裝置，其中該歸屬網路的該節點包括一歸屬用戶伺服器（HSS）或認證、授權、和計費（AAA）伺服器。

圖式

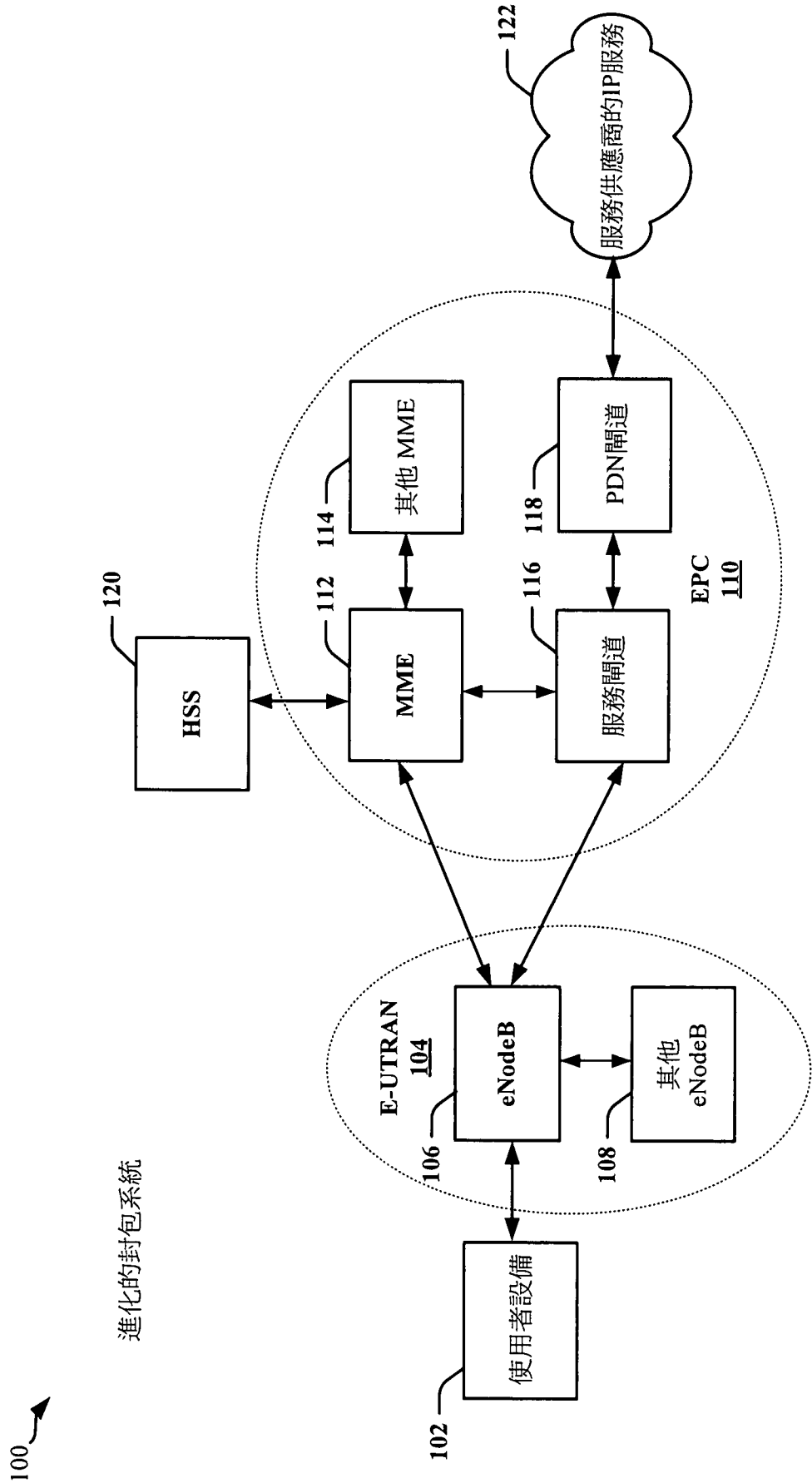


圖 1

200

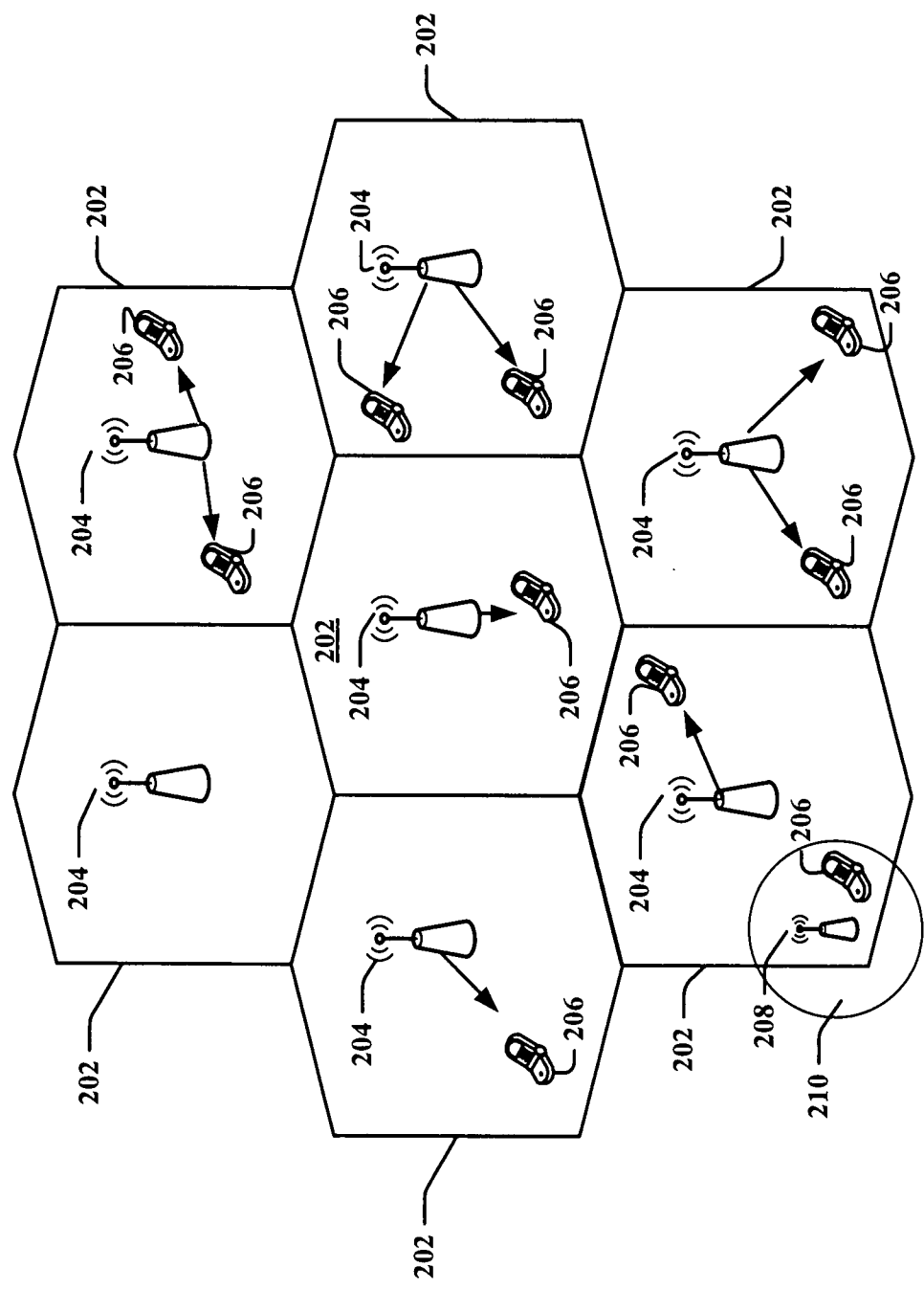


圖 2

300

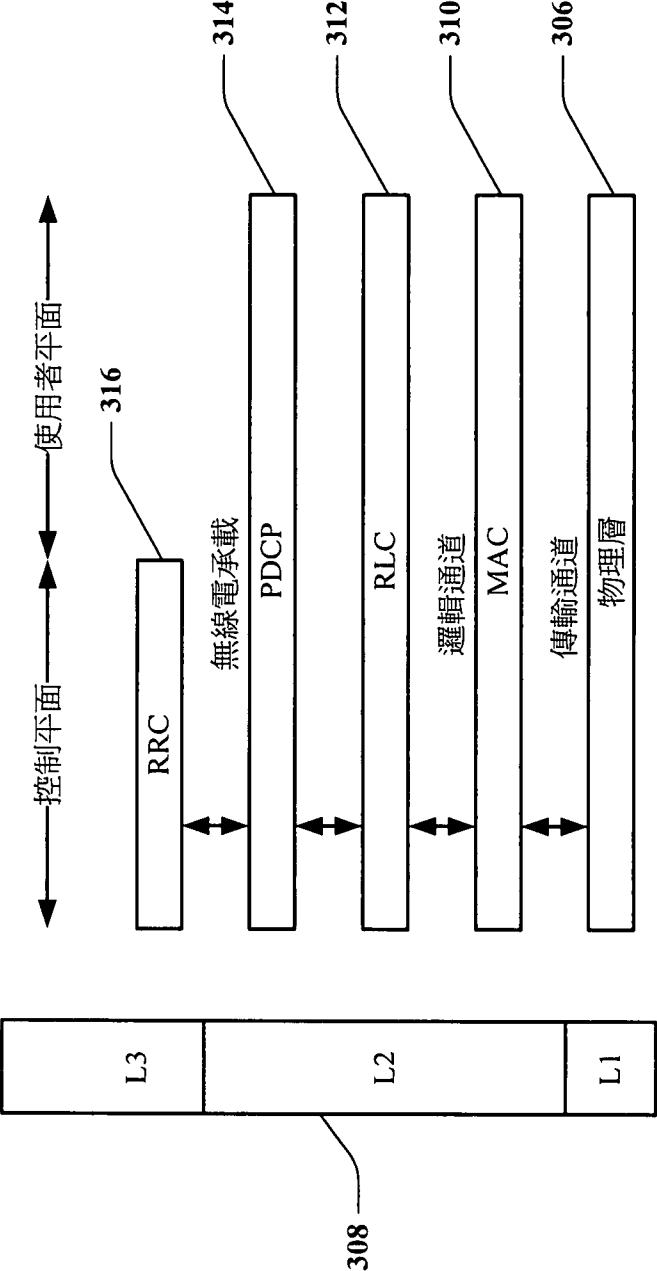


圖 3

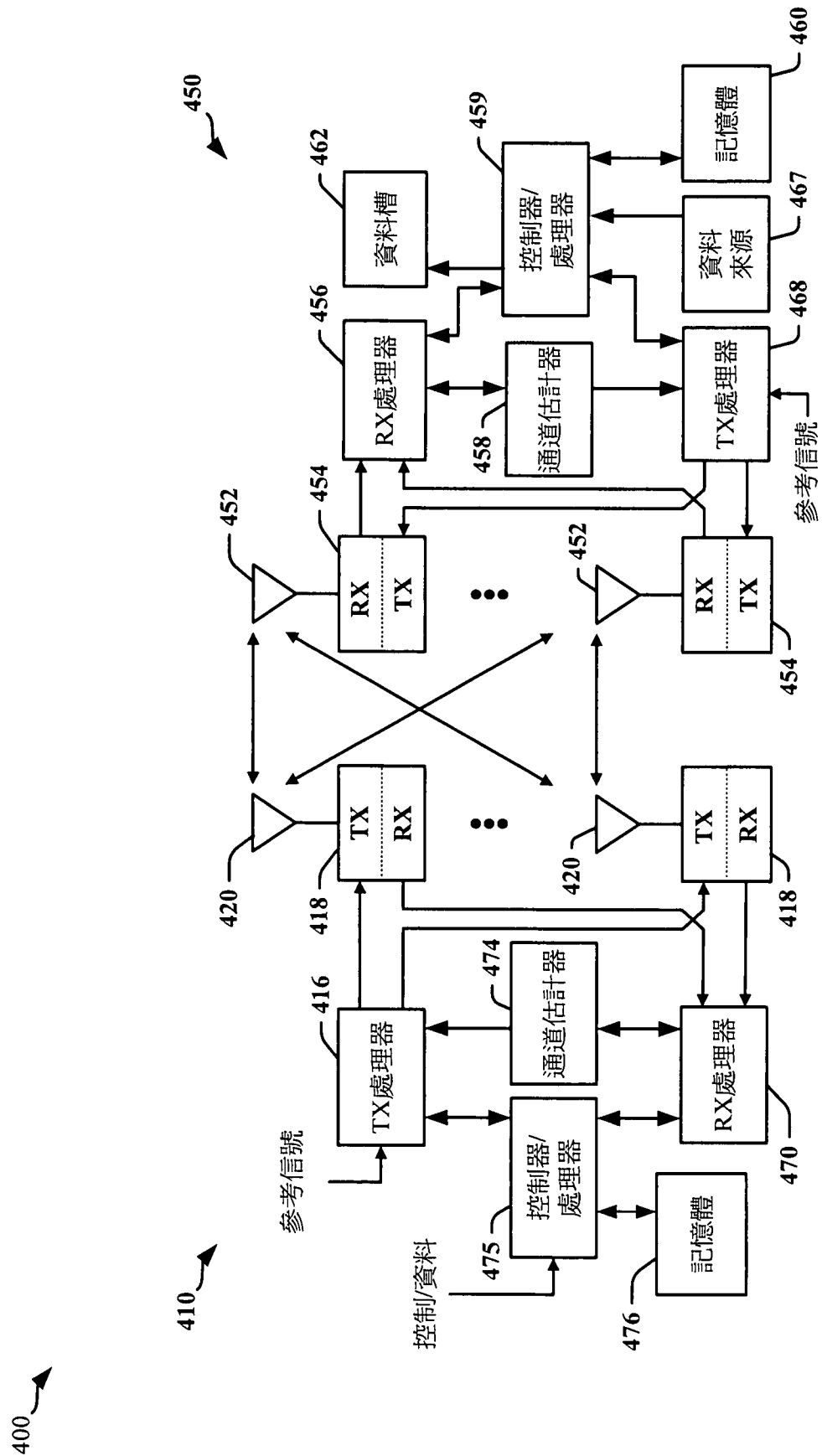


圖 4

500

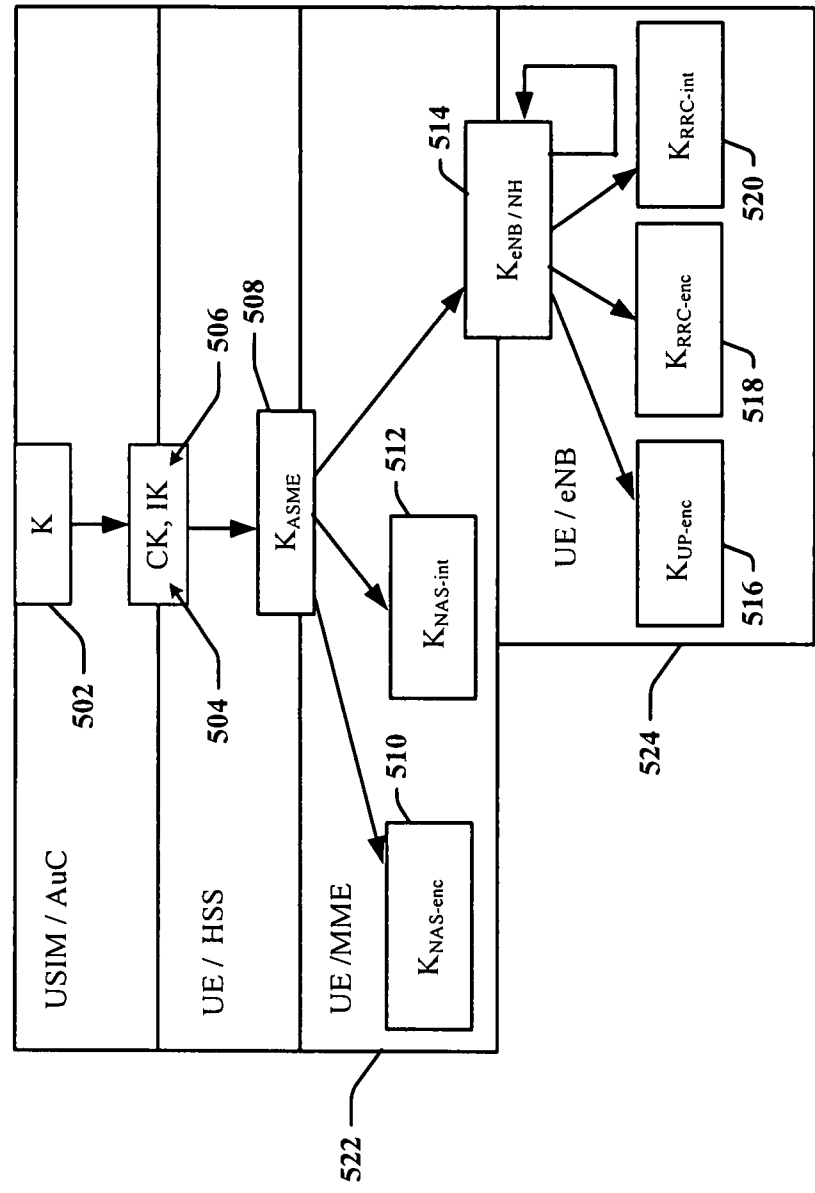


圖 5

600 ↗

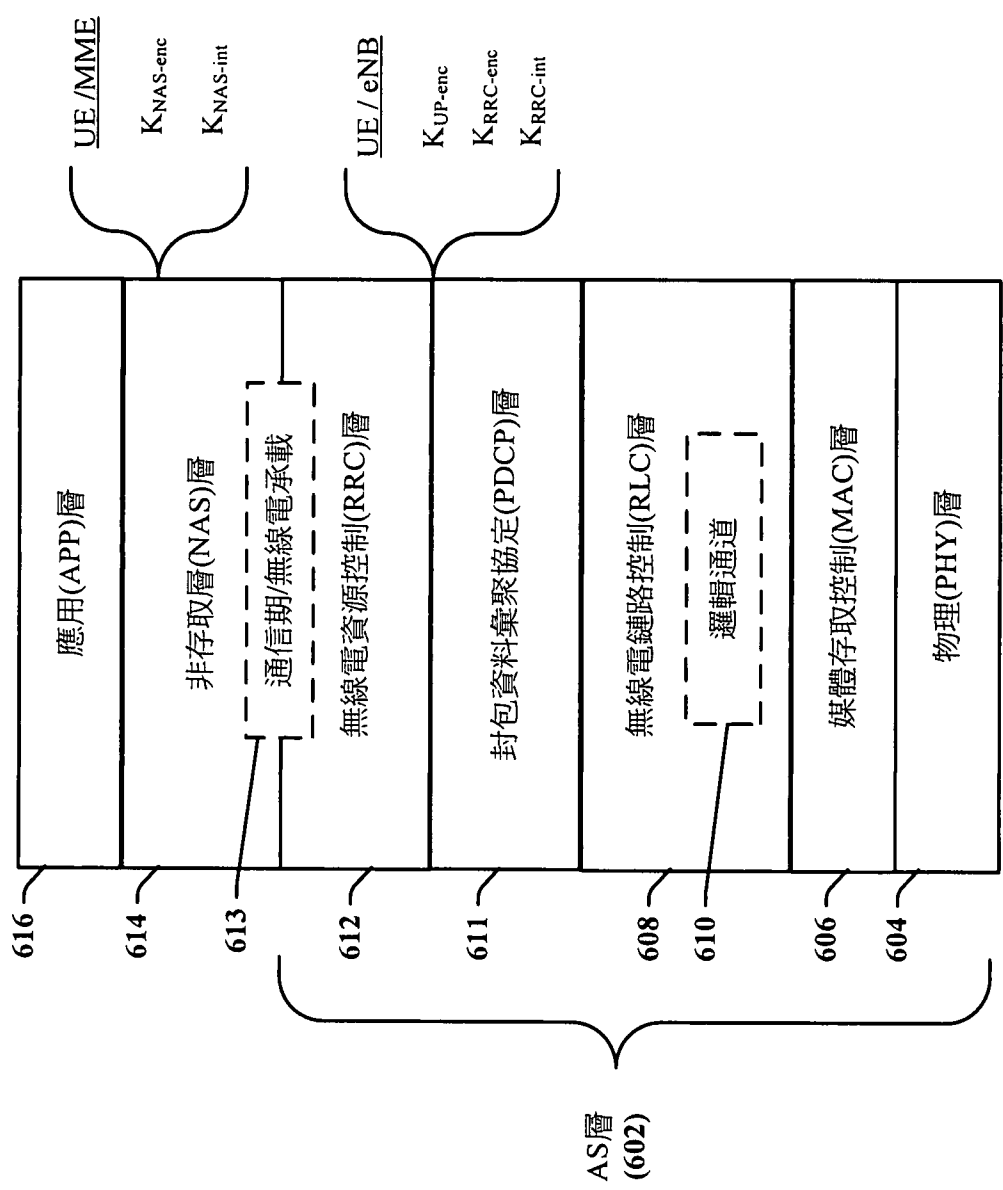


圖 6

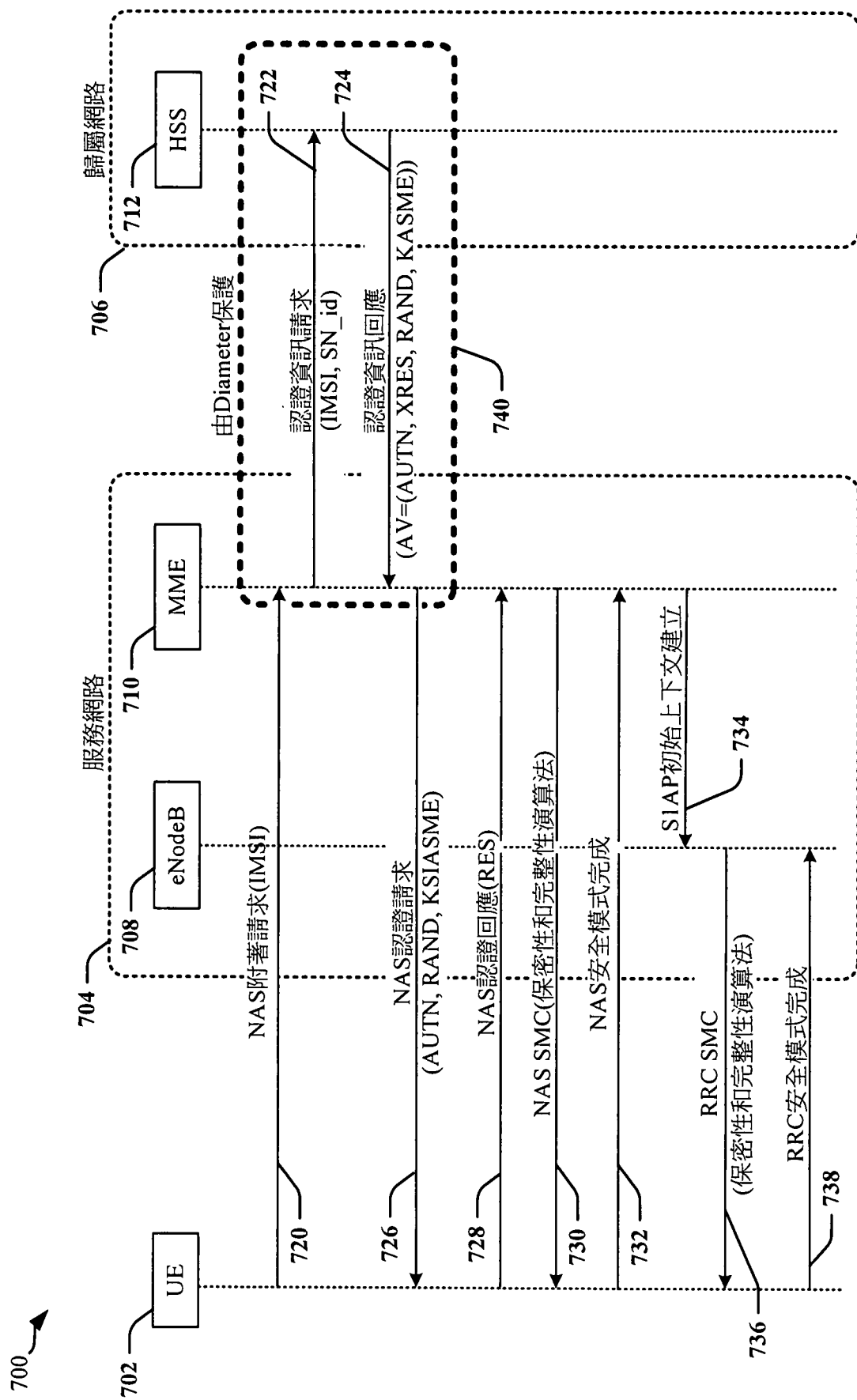


圖 7

800

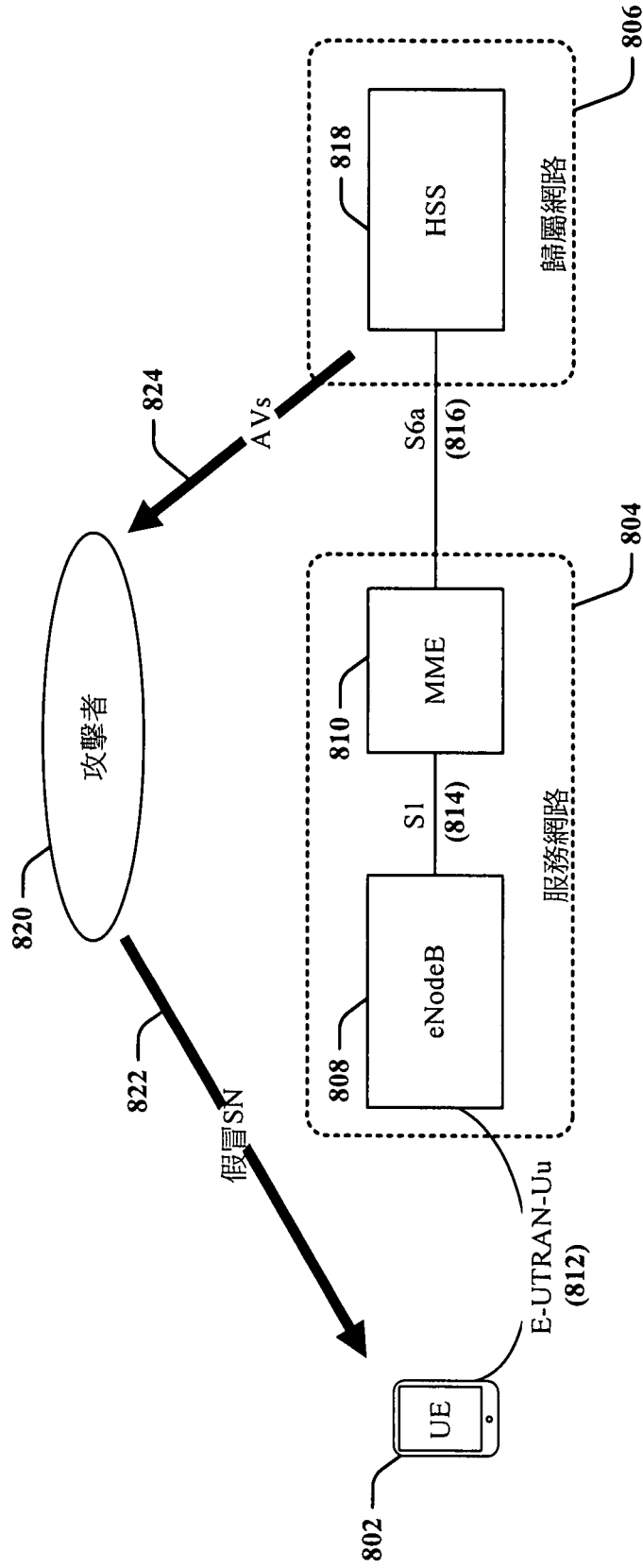


圖 8

900

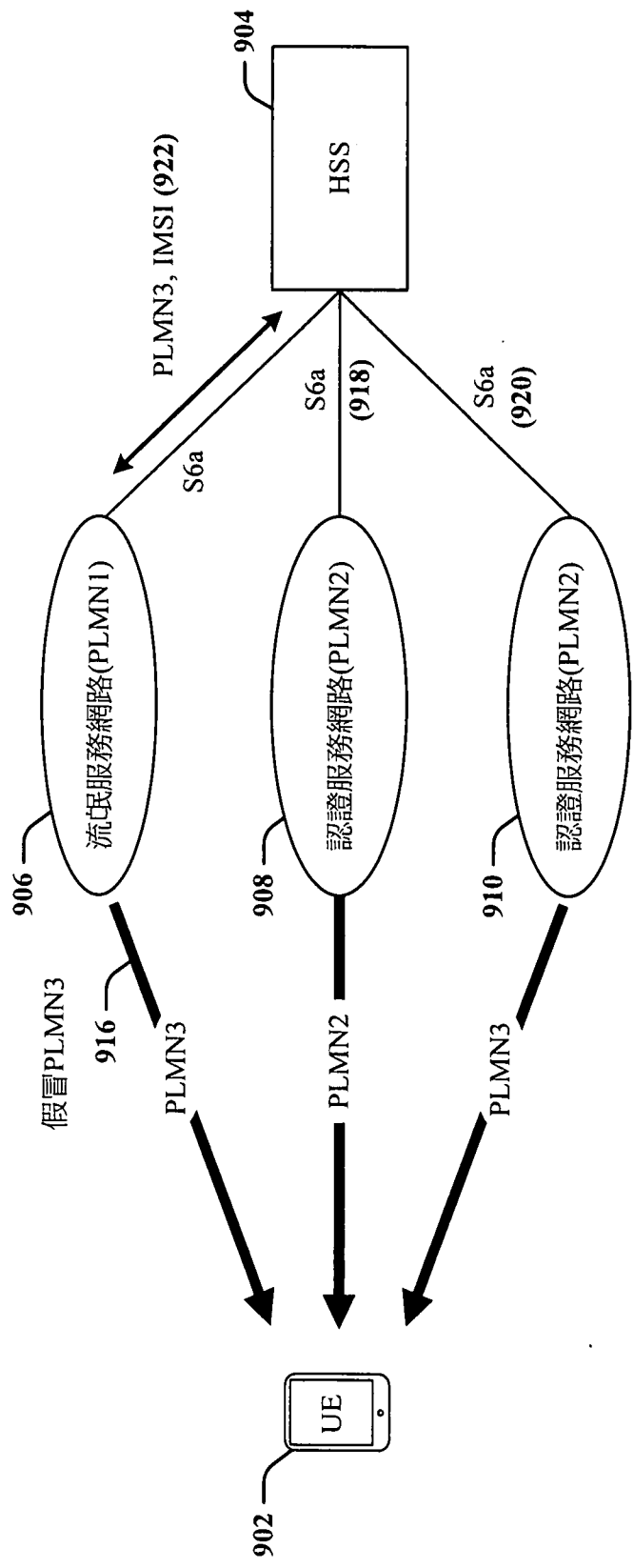


圖 9

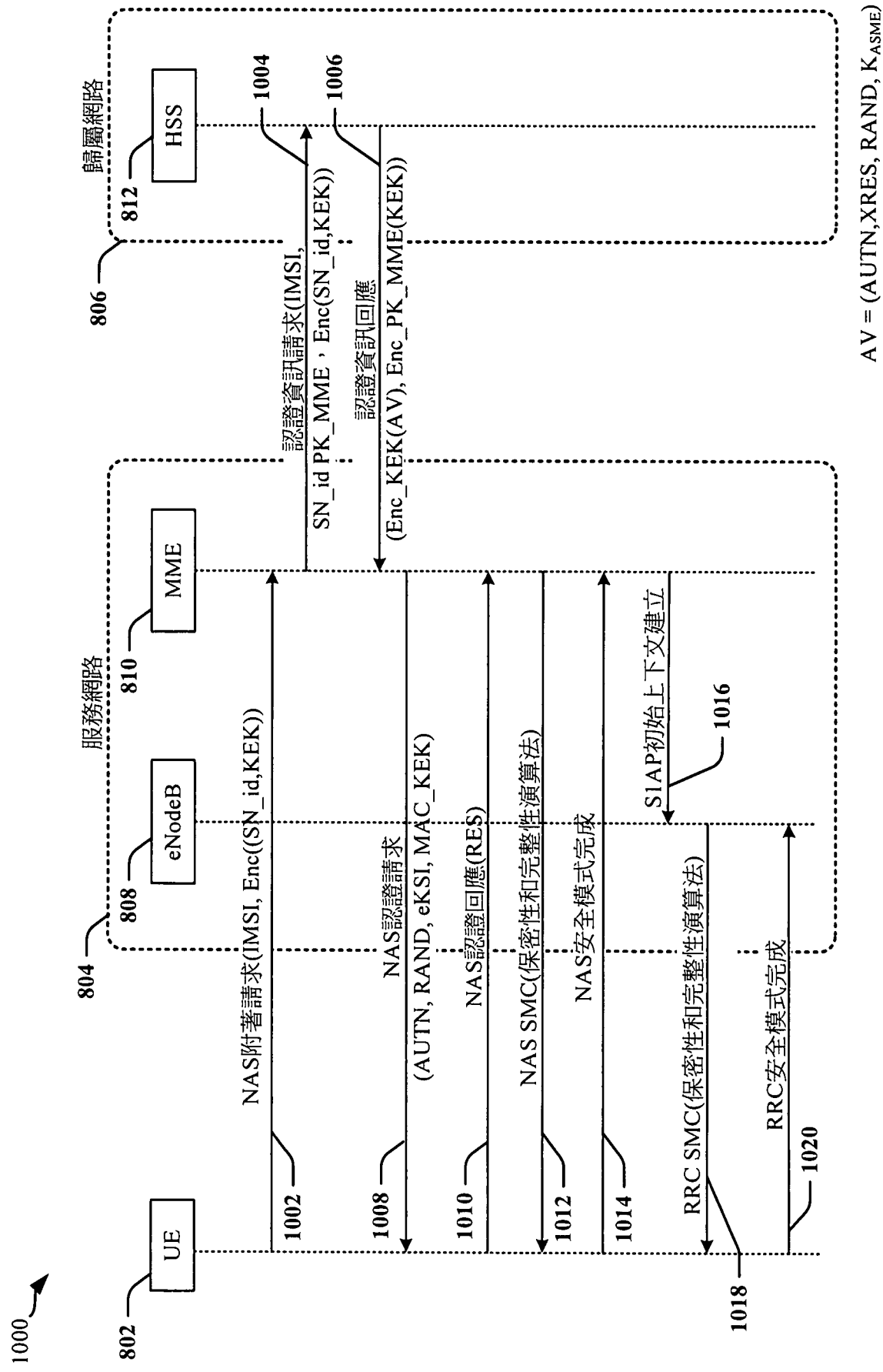


圖 10

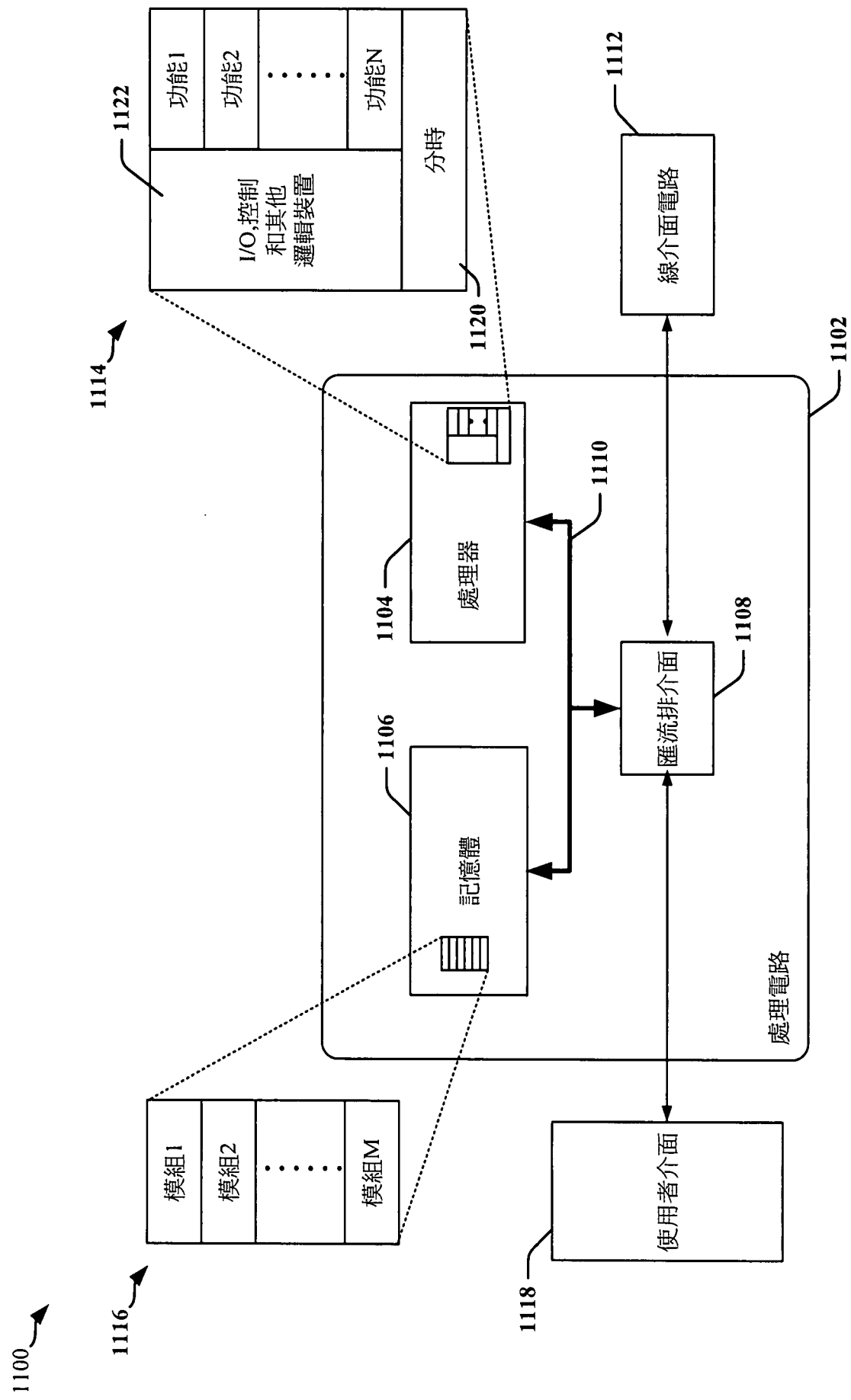


圖 11

1200

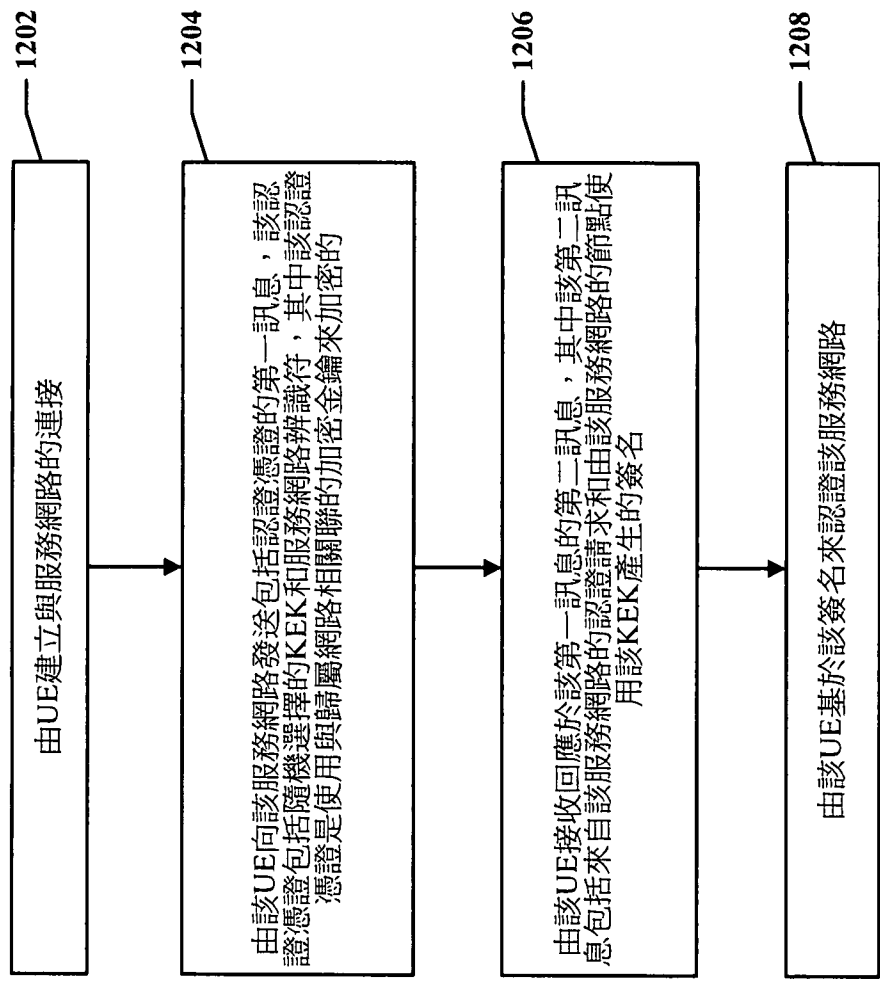


圖 12

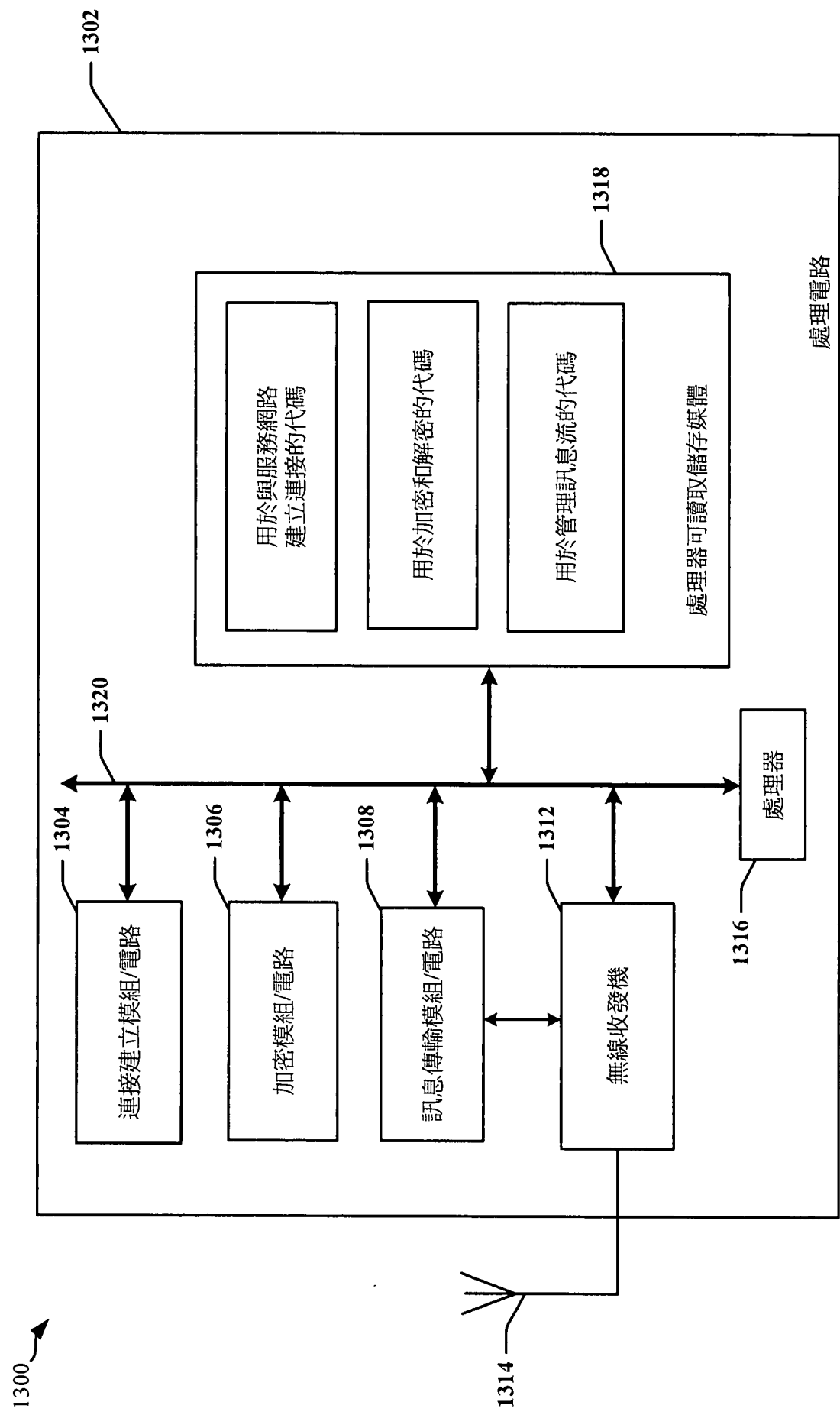


圖 13

1400

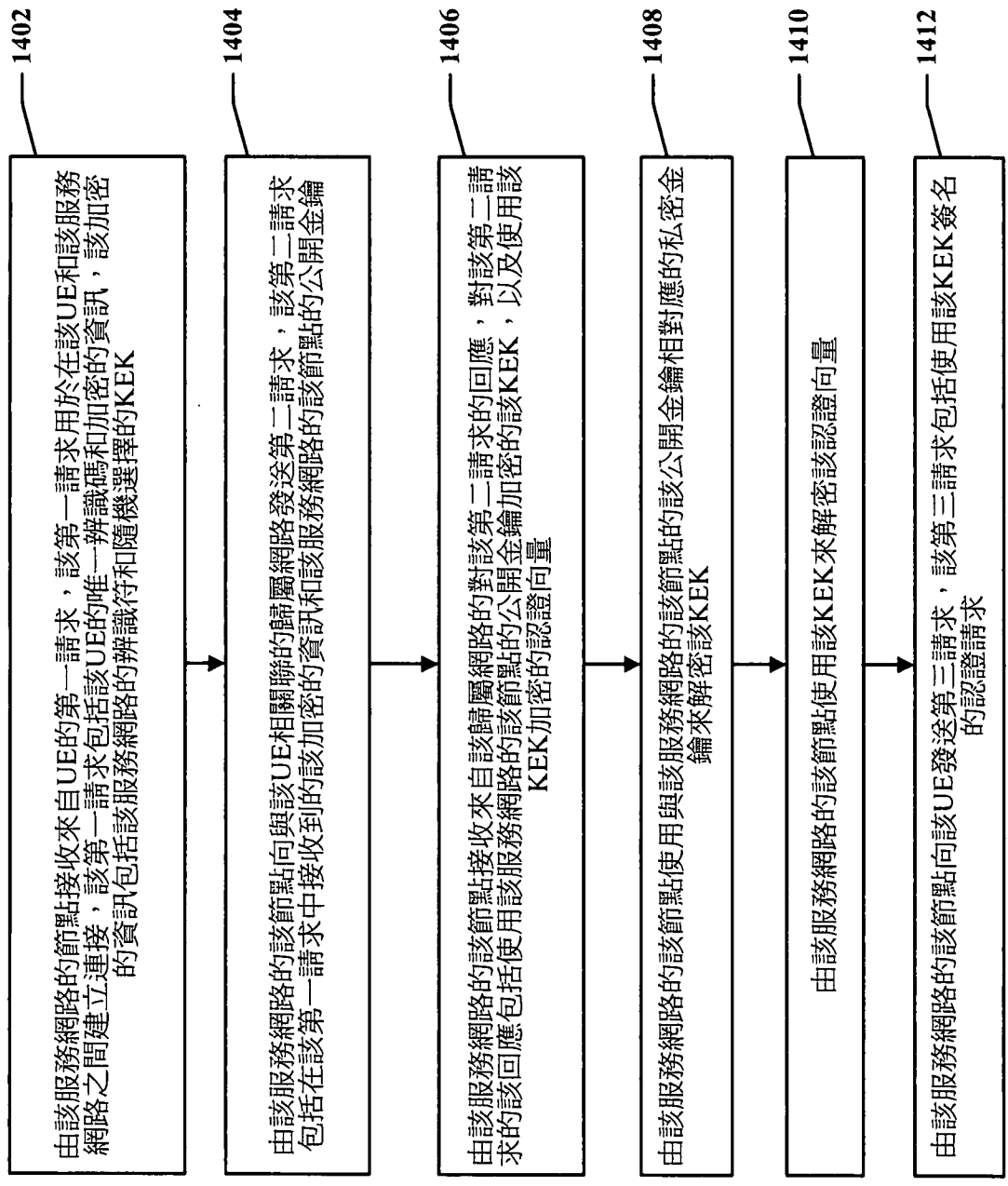


圖 14

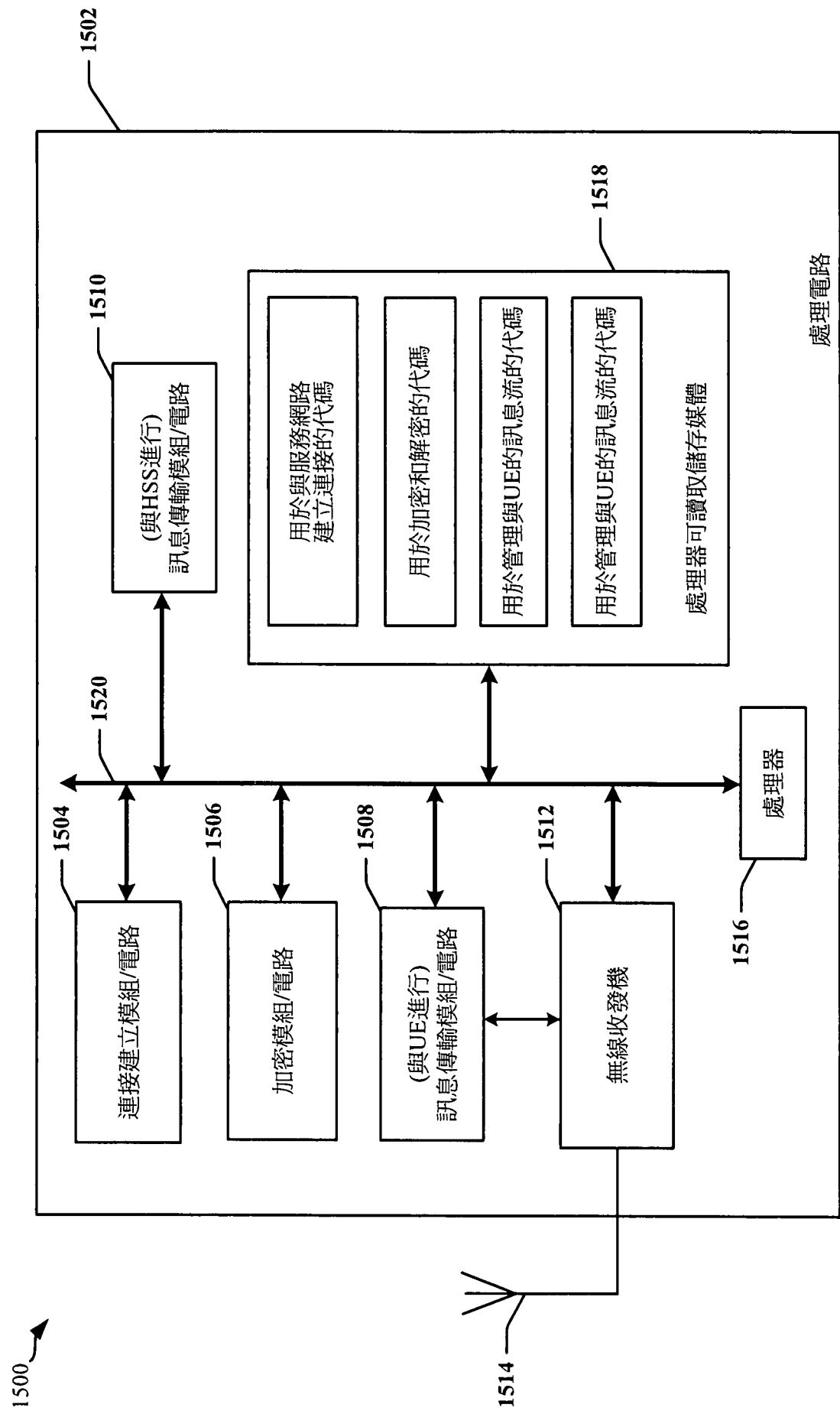


圖 15

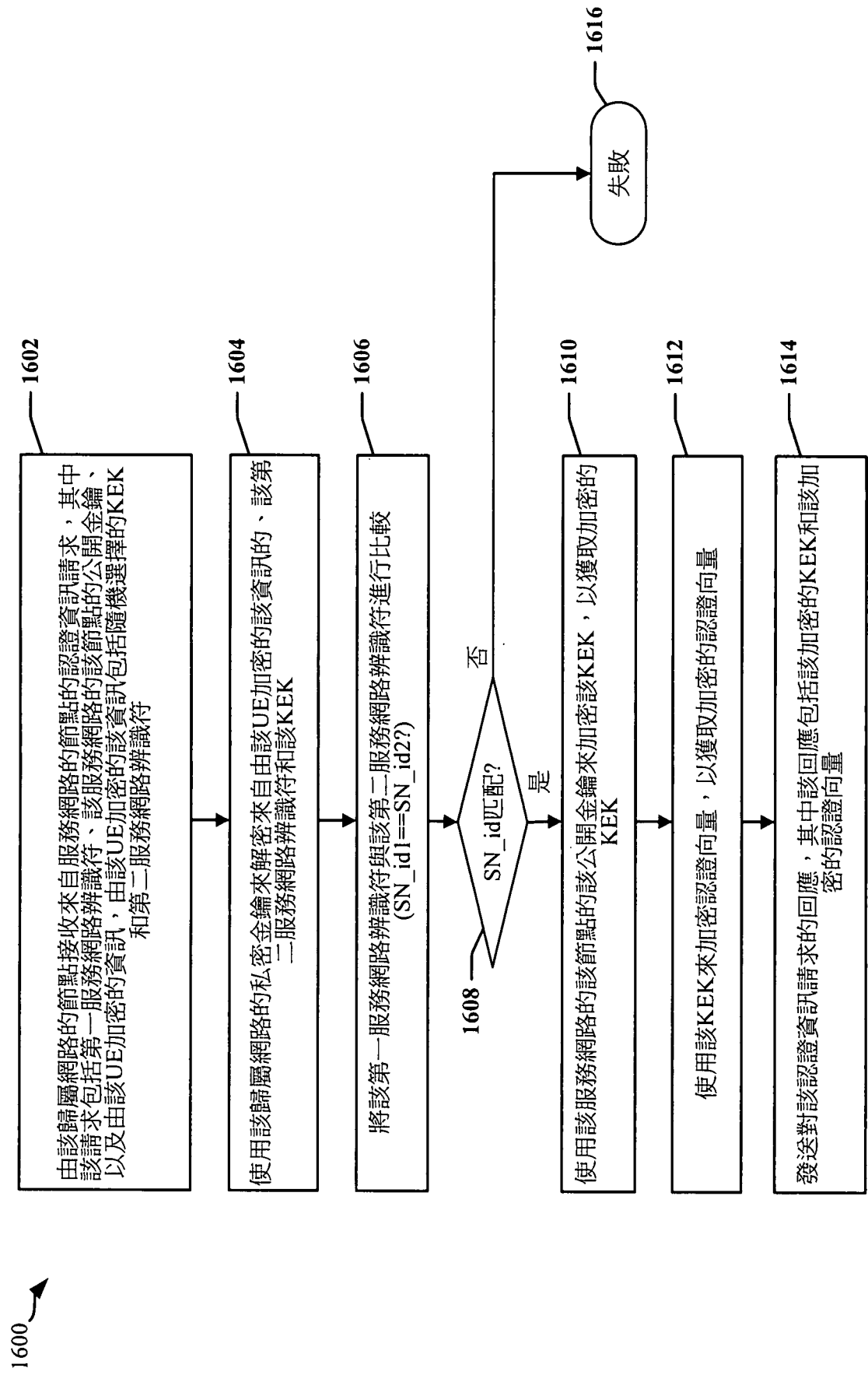


圖 16

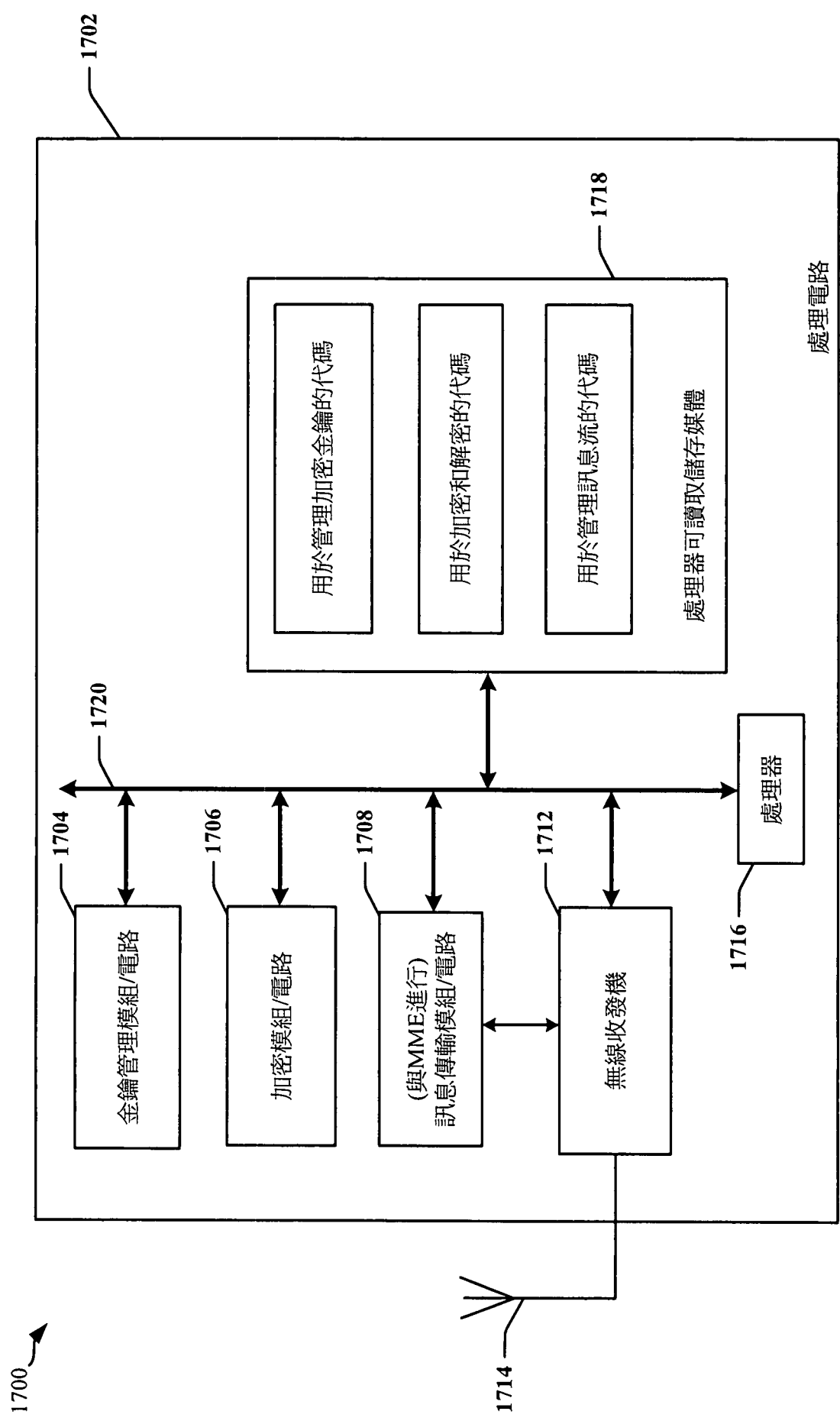


圖 17