I469555

(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 I469555 B**

(45)公告日： 中華民國 104 (2015) 年 01 月 11 日

(21)申請案號：097140551 (22)申請日： 中華民國 97 (2008) 年 10 月 22 日

(51)Int. Cl.： ***H04B7/00 (2006.01)*** ***H04L9/00 (2006.01)***

(30)優先權：2007/10/25 美國 60/982,698

(71)申請人：內數位專利控股公司 (美國) INTERDIGITAL PATENT HOLDINGS, INC. (US)
美國

(72)發明人：山卡爾 索馬桑德朗 SHANKAR SOMASUNDARAM (IN)；拉傑 普利塔 穆克吉 RAJAT PRITAM MUKHERJEE (IN)

(74)代理人：蔡清福

(56)參考文獻：

EP 1248487A2 US 2004/0258019A1

US 2007/0171857A1

審查人員：蔡穎欣

申請專利範圍項數：12 項 圖式數：6 共 48 頁

(54)名稱

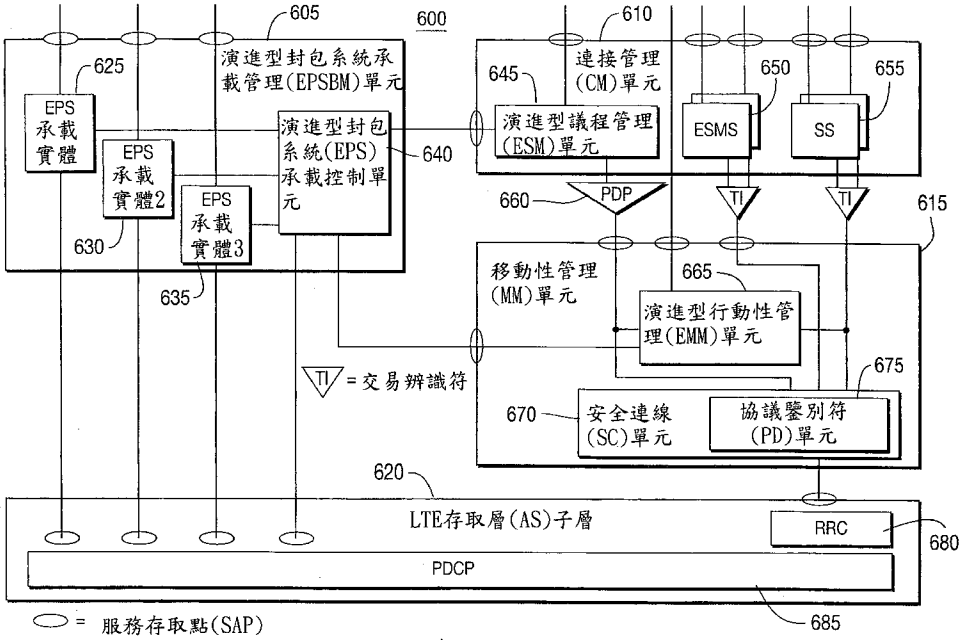
長期演進行動單元非存取層架構及協議增強

NON-ACCESS STRATUM ARCHITECTURE AND PROTOCOL ENHANCEMENTS FOR LONG TERM EVOLUTION MOBILE UNITS

(57)摘要

公開了一種執行長期演進(LTE)無線傳輸/接收單元(WTRU)中非存取層(NAS)(層 3)的處理的方法和設備，所述方法和設備允許 NAS 協定層將 L3 訊息路由到正確的 NAS 實體，並為新的 NAS 訊息類型和資訊元素進行編碼。提出了確保 NAS 安全性的新架構。當產生 NAS 訊息時，基於 NAS 訊息的協定鑒別符(PD)、NAS 訊息的標頭中的指示符欄位元、NAS 訊息的類型、NAS 安全性狀態變數以及根據上層協定的指示中的至少其中之一來做出是否對 NAS 訊息進行加密、解密及/或完整性檢查的決定。所述 NAS 安全性狀態變數指示 NAS 安全性當前是否處於有效狀態並且可以包括一個位元。

A method and apparatus performs processing of the non-access stratus (NAS) layer (layer 3) in long term evolution (LTE) wireless transmit/receive units (WTRUs), which allows the NAS protocol layer to route layer 3 messages to the correct NAS entity, and to encode new NAS message types and information elements. A new architecture is presented that enables NAS security. When a NAS message is generated, a determination is made as to whether or not to cipher, de-cipher and/or integrity check the NAS message based on at least one of a protocol discriminator (PD) of the NAS message, an indicator field in a header of the NAS message, the type of the NAS message, a NAS security state variable, and an indication by an upper layer protocol. The NAS security state variable indicates whether NAS security is currently active or not and may comprise one bit.



第6圖

600・・・非存取層層3架構

605・・・演進型封包系統承載管理單元

610・・・連接管理單元

615・・・移動性管理單元

620・・・長期演進存取層子層

625・・・演進型封包系統承載實體1

630・・・演進型封包系統承載實體2

635・・・演進型封包系統承載實體3

640・・・演進型封包系統承載控制單元

645・・・演進型議程管理單元

650・・・演進型短訊息服務實體

655・・・補充服務實體

660、PDP・・・封包資料協定

665・・・演進型行動性管理單元

670・・・安全連線單元

675・・・協議鑒別符單元

680・・・無線電資源控制

685・・・封包資料彙聚協定

EPS・・・演進型封包系統

ESMS・・・演進型短訊息服務

SS・・・補充服務

LTE・・・長期演進

RRC・・・無線電資源控制

PDCP・・・封包資料彙聚協定

PDP・・・封包資料協定

TI・・・交易辨識符

公告本

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：097140551

※ 申請日期：97 年 10 月 22 日　　※IPC 分類：H04B 7/00 (2006.01)
H04L 9/00 (2006.01)

一、發明名稱：（中文/英文）

長期演進行動單元非存取層架構及協議增強/Non-Access Stratum Architecture And Protocol Enhancements for Long Term Evolution Mobile Units

二、中文發明摘要：

公開了一種執行長期演進（LTE）無線傳輸/接收單元（WTRU）中非存取層（NAS）（層 3）的處理的方法和設備，所述方法和設備允許 NAS 協定層將 L3 訊息路由到正確的 NAS 實體，並為新的 NAS 訊息類型和資訊元素進行編碼。提出了確保 NAS 安全性的新架構。當產生 NAS 訊息時，基於 NAS 訊息的協定鑒別符（PD）、NAS 訊息的標頭中的指示符欄位元、NAS 訊息的類型、NAS 安全性狀態變數以及根據上層協定的指示中的至少其中之一來做出是否對 NAS 訊息進行加密、解密及/或完整性檢查的決定。所述 NAS 安全性狀態變數指示 NAS 安全性當前是否處於有效狀態並且可以包括一個位元。

三、英文發明摘要：

A method and apparatus performs processing of the non-access stratus (NAS) layer (layer 3) in long term evolution (LTE) wireless transmit/receive units (WTRUs), which allows the NAS protocol layer to route layer 3 messages to the correct NAS entity, and to encode new NAS message types and information elements. A new architecture is presented that enables NAS security. When a NAS message is generated, a determination is made as to whether or not to cipher, de-cipher and/or integrity check the NAS message based on at least one of a protocol discriminator (PD) of the NAS message, an indicator field in a header of the NAS message, the type of the NAS message, a NAS security state variable, and an indication by an upper layer protocol. The NAS security state variable indicates whether NAS security is currently active or not and may comprise one bit.

四、指定代表圖：

(一)本案指定代表圖為：第（6）圖。

(二)本代表圖之元件符號簡單說明:

600	非存取層層 3 架構
605	演進型封包系統承載管理單元
610	連接管理單元
615	移動性管理單元
620	長期演進存取層子層
625	演進型封包系統承載實體 1
630	演進型封包系統承載實體 2
635	演進型封包系統承載實體 3
640	演進型封包系統承載控制單元
645	演進型議程管理單元
650	演進型短訊息服務實體
655	補充服務實體
660、PDP	封包資料協定
665	演進型行動性管理單元
670	安全連線單元
675	協議鑒別符單元
680	無線電資源控制
685	封包資料彙聚協定
EPS	演進型封包系統
ESMS	演進型短訊息服務
SS	補充服務
LTE	長期演進

RRC	無線電資源控制
PDCP	封包資料彙聚協定
PDP	封包資料協定
TI	交易辨識符

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本申請涉及無線通訊。

【先前技術】

第三代合作夥伴計畫（3GPP）長期演進（LTE）專案的當前努力方向是引進與 LTE 設置和配置相關的新技術、新架構和新方法，以提供改進的頻譜效率、減少的延遲、無線電資源的更好利用，從而以更低的成本帶來更快捷的用戶體驗以及更豐富的應用和服務。

LTE 層 3（L3）架構可以被認為是用於能夠實現通用封包無線電服務（GPRS）的無線傳輸/接收單元（WTRU）（即基地台）的現有 L3 架構的演進。LTE 定義了新的行動性管理（MM）概念（例如以跟蹤區域取代路由區域的概念）以及新的 MM 過程（例如多個跟蹤區域可以在跟蹤區域更新過程中被分配）。這些新的過程將由新的 L3 協議（例如演進型行動性管理（EMM）和演進型議程管理（ESM））來進行更詳細的描述，這將是 LTE 非存取層（NAS）的一部分。這些新的協定實體是 GPRS 行動性管理（GMM）、議程管理（GMM）等等的 LTE 等價物。

此外，作為這一演進過程的一部分，3GPP 將在 LTE 中使用不同的安全性架構，而不在通用行動電信系統（UMTS）和用於行動通訊（GSM）的全球系統中使用。為了進行比較，UMTS 認證和密鑰協議（AKA）過程（在封包交換（PS）區域中）可被認為是用於新的 LTE 過程的

基準。當前的 UMTS AKA 過程和新的 LTE 安全性架構現在將被簡要地描述。

UMTS AKA 和加密過程被擴展到多個協定層，並使用 NAS 和無線電資源控制（RRC）發信兩者來共同完成它們的目標。簡言之，WTRU 的識別和認證經由 NAS 發信來完成。一旦在 NAS 級別的認證被完成，加密及/或完整性保護就由網路使用安全性模式指令來啟動，該安全性模式指令是 RRC 訊息。一旦使用安全性模式指令啟動了安全性，WTRU 中的 NAS 層首先使用在 GMMAS 服務存取點(SAP)（被定義在 GMM 與 AS 之間）上的 GMMAS-SECURITY-RESPONSE（GMMAS-安全性-回應）原語向存取層（AS）傳遞加密密鑰（CK）和完整性密鑰（IK)。RRC 接收這些密鑰並使用 CRLC-CONFIG 原語(在 RRC 與 RLC 之間的 C-SAP 上)和 CMAC-CONFIG 原語(在 RRC 與 MAC 之間的 C-SAP 上）將所述密鑰傳遞到無線電鏈結控制（RLC）和媒體存取控制（MAC）上。C-SAP 是用於 RRC 與較低層之間的 C-平面發信的服務存取點。實際的加密和完整性保護通常在 RLC 中執行，但是在透明的 RLC 模式業務的情況中則在 MAC 中執行。較低層（即 MAC/RLC）負責確保供上層使用的訊息（例如 L3 NAS 訊息）已經被正確地進行了完整性保護及/或加密。如果沒有，則較低層忽略/丟棄該訊息。

針對 LTE 的用於安全性的完全不同的架構已經被提出。主要區別在於現有兩個安全級別-NAS 安全性和 AS 安

全性，而不是單一的安全性層（即在 MAC/RLC 中）。NAS 安全性在行動性管理實體（MME）（即核心網路）中終止，而 AS 安全性在基地台（即 e 節點-B）中終止。簡言之，AKA 過程在 NAS 中完成，NAS 安全性密鑰在完成後首先被導出，而 AS 安全性參數以密碼分離的方式（即知道 AS 密鑰不允許攻擊者確定 NAS 密鑰）從 NAS 密鑰導出。這一決定的理由是在 LTE 中，一方可能在易受攻擊的位置（例如歸屬節點-B）存在基地台，以及由於 RRC（以及由此的安全性）在基地台中被終止，這被認為是安全性風險。因此需要兩個安全性級別。

第 1 圖示出了常規 LTE L3 標頭 100 的結構。LTE L3 標頭 100 的第一個八位元組包括交易辨識符或跳躍指示符欄位 105 和協議鑒別符（PD）欄位 110。LTE L3 標頭 100 的第二個八位元組包括訊息類型欄位 115。LTE L3 標頭 100 的附加八位元組可以包括根據需要的其他資訊元素 120。如上所描述，新的 L3 協定實體已經被提出（例如 EMM 和 ESM）。然而，當前的 LTE L3 標頭 100 不支援這些新的協定。特別地，第 1 圖的 LTE L3 標頭 100 中的 PD 欄位 110 被增強，以根據選項來區分這些新的協定。

第 2 圖示出了第 1 圖的 LTE L3 標頭 100 的 PD 欄位 110。參見第 1 圖和第 2 圖，LTE L3 標頭 100 的第一個八位元組的最後 4 位元（4321）構成 PD 欄位 110，其由 NAS 的 MM 子層中的路由實體使用以將 L3 訊息路由到合適的 NSA 實體（例如當前的 MM/GMM/SM），其中該 L3 訊息

包括 LTE L3 標頭 100。

第 3 圖中示出了僅 PS 的 UMTS WTRU 的常規 NAS 架構 300。NAS 架構 300 包括無線電存取承載管理（RABM）單元 305、連接管理（CM）單元 310、行動性管理（MM）單元 315 以及存取層（AS）子層 320。RABM 單元 305 包括多個無線電存取承載（RAB）實體 325、330 和 335，以及 RAB 控制單元 340。CM 單元 310 包括議程管理（SM）單元 345、GPRS 短訊息服務（GSMS）實體 350 以及補充服務（SS）實體 355。封包資料協定（PDP）360 被用作 CM 單元 310 與 MM 單元 315 之間的介面。MM 單元 315 包括 GPRS MM（GMM）單元 365 和 PD 單元 370。MM 單元 315 和 RABM 單元 305 介面都具有 AS 子層 320，該 AS 子層 320 包括無線電資源控制器（RRC）375、廣播多播控制器（BMC）380 以及封包資料彙聚協定（PDCP）385。AS 子層 320 向 MM 單元 315 和 RABM 單元 305 提供服務。MM 單元 315 向 CM 單元 310 的實體提供服務。

RAB 控制單元 340 增加、改變、刪除及/或重新配置 RAB 實體 325、330 和 335。PD 單元 370 用於將 NAS 訊息資訊元素（IE）路由到不同的 NAS 實體。SM 單元 345 向 RABM 單元 305 提供服務並使用 MM 單元 315 的服務。除了使用來自 GMM 單元 365 的服務之外，GSMS 實體 350 與用於 GSM 中的 GPRS 服務的 SMS 實體相同。除了使用來自 PS 發信連接的服務之外，SS 實體 355 與來自非 GPRS 服務的一方相同。RABM 單元 305 隱藏 RAB 的概念，當

PDP 上下文處於活動狀態時該 RAB 可以被啟動/釋放。如果終端中的上鏈（UL）資料將在已經被釋放的 RAB（網路服務存取點辨識符（NSAPI））上被發送，那麼 RABM 單元 305 將在 GMM 單元 365 中觸發服務請求過程。

通常，NAS 訊息 IE 以類型/長度/數值（TLV）格式進行編碼。如第 4 圖所示，NAS 訊息 IE 屬於 5 種類型的 IE 405、410、415、420 和 425 中的一種。如第 4 圖所示，IE 405 僅具有類型（T）格式，IE 410 僅具有數值（V）格式，而 IE 415 具有類型和數值（TV）格式，IE 420 具有長度和數值（LV）格式，而 IE 425 具有類型、長度和數值（TLV）格式。如第 4 圖所示，IE 指示符（類型）存在於 IE 405、415 和 425 中，但不存在於 IE 410 和 420 中。長度指示符存在於 IE 420 和 425 中，但不存在於 IE 405、410 和 415 中。數值指示符存在於 IE 410、415、420 和 425 中，但不存在於 IE 405 中。

使用第 3 圖的 NAS 架構 300 具有的一些問題在於所建議的新的 NAS 訊息不具有為了被識別而被定義的任意訊息類型。另外，一些期望的新的 NAS IE 沒有為其編碼而定義的格式。此外，第 3 圖中示出的 NAS 實體不支援安全性（即難以使用當前 NAS 架構來實現 LTE NAS 中的安全性）。

另外，在 NAS 架構 300 中，所建議的用於 LTE 的加密演算法是區塊加密，即它們藉由使用 CK 和待加密的協定資料單元（PDU）的長度的指示來產生密鑰串流區塊來工作，所述密鑰串流區塊的長度等於未加密的 PDU 的長度。

然後所述密鑰串流區塊被逐位增加（通常）到未加密的PDU，以產生加密的 PDU。該過程也被用在接收器以產生用於解密的同樣的密鑰串流區塊。接著該密鑰串流區塊被逐位增加到接收到的加密的 PDU。

在 LTE 中，NAS 訊息的加密已經被認同。因此，NAS 層必須向加密演算法指示待加密的 L3 NAS PDU 的長度。現今並不存在用於 NAS 進行這一過程的功能性。

最後，如果允許 MME 的再定位，那麼在切換過程中 MME 再定位可能可以發生。第 5 圖中示出了用於執行 MME 的再定位的切換過程的一個實例。當前不存在無線電鏈結失敗和 MME 間的切換之後對 NAS 序列號（SN）和超訊框號（HFN）的處理而定義的過程。

【發明內容】

本申請描述 LTE WTRU 中的 NAS 層（L3）的特徵，由此允許所述 NAS 協定層將層 3 訊息路由到正確的 NAS 實體，並對新的 NAS 訊息類型和資訊元素進行編碼。提出了確保 NAS 安全性的新架構。當產生 NAS 訊息時，基於所述 NAS 訊息的協定鑒別符（PD）、所述 NAS 訊息的標頭中的指示符欄位、所述 NAS 訊息的類型、NAS 安全性狀態變數以及根據 RRC 協定的指示中的至少其中之一來做出是否對所述 NAS 訊息進行加密、解密及/或完整性檢查的決定。所述 NAS 安全性狀態變數指示當前 NAS 安全性是否被啟動，並且可以包含一個位元。

本發明的有益效果包括：允許所述 NAS 協定層將 L3

訊息路由到正確 LTE NAS 實體（例如 EMM 和 ESM）。允許新的 NAS 訊息類型和新的 NAS IE 的編碼。提供了新的 NAS 架構以確保 NAS 安全性並允許對用於產生相等長度的加密密鑰串流的 NAS PDU 的長度的確定。此外，允許所述 NAS 層在無線電鏈結失敗和切換後處理 SN 和 HFN。

【實施方式】

下文提及的“無線傳輸/接收單元（WTRU）”包括但不局限於使用者設備（UE）、行動站、固定或行動使用者單元、傳呼機、蜂窩電話、個人數位助理（PDA）、電腦或能夠在無線環境中操作的任何其他類型的使用者設備。下文提及的“基地台”包括但不局限於節點-B、站點控制器、存取點（AP）或能夠在無線環境中操作的任何其他類型的周邊設備。

層 3 協議鑒別符（PD）欄位的增強

參見第 1 圖，LTE L3 標頭 100 中的 L3 PD 欄位 110 可以被增強，以使得 L3 PD 欄位 110 中的位元的特定組合指示 LTE LE 標頭 100 之後的 L3 訊息是上層 LTE L3 訊息(例如 EMM、ESM)。

術語 EMM 和 ESM 被用於描述 LTE MM 和 SM 實體及協定、以及它們的相關聯的功能。如果任意附加的實體/協定在用於 LTE 的 NAS 層中被定義/修改，它們各自的協議也可以被增加到 L3 PD 欄位。然而，如第 2 圖中所示，很少位元的組合可以用於這一目的。因此，下面的選項可以被實現：

1)定義備用的 PD 值“0111”和“1101”以表示 EMM 和 ESM 協定（以任意順序）；

2）擴展 PD 欄位為一個八位元組（或者更多）並將（這一增加的 PD 欄位可以採用的可用值的）兩個值映射到 EMM 和 ESM 協議；

3）重新使用一些現有的 PD 值（例如用於 GMM 訊息的 1000），以指示 EMM 和 ESM 協議。

訊息類型的增強的描述

參見第 1 圖，LTE L3 標頭 100 的第二個八位元組包括訊息類型欄位 115。這一八位元組的不同值映射到由協定鑒別符欄位 110 識別的協定層的不同訊息。

為了定義期望用於 LTE 的新的 L3 NAS 訊息，訊息類型欄位 115 中的附加值可以被分配用於如下：

1）跟蹤區域更新請求；

2）跟蹤區域更新接受；

3）跟蹤區域更新完成；

4）跟蹤區域更新拒絕；

5）NAS 安全性模式指令；

6）NAS 安全性模式指令完成；以及

7）NAS 安全性模式指令失敗。

NAS 訊息中的新的完整性檢查（IC）資訊元素

為了對 NAS 訊息進行完整性檢查，新的 NAS 完整性檢查（IC）IE 可以被追加到每個 NAS 訊息。接收器將該接收到的 IE 的值與其自身的計算結果進行比較。由於 IC 位

元的長度可能將被固定（因為它是已知演算法的輸出），IC IE 可以被編碼為類型 3 NAS 訊息 IE（僅類型和數值（TV)），因為數值部分的長度是固定的。可替換地，它可以被編碼為類型 2 或某些其他類型。新的 IE 辨識符可以被定義以識別 NAS IC IE。

用於保護 NAS 層的新的架構

以下描述的不同架構用於保護 NAS 層。

用於安全性的 NAS 實體/協定

第 6 圖示出了新的 NAS L3 架構 600 的實例，其可以在 WTRU（即行動站）內部駐留。NAS L3 架構 600 包括演進型封包系統承載管理（EPSBM）單元 605、CM 單元 610、MM 單元 615 以及 LTE AS 子層 620。EPSBM 單元 605 包括多個演進型封包系統（EPS）承載實體 625、630 和 635，以及 EPS 控制單元 640。CM 單元 610 包括演進型議程管理（ESM）單元 645、演進型短訊息服務（ESMS）實體 650、以及補充服務（SS）實體 655。PDP 660 被用作 CM 單元 610 與 MM 單元 615 之間的介面。MM 單元 615 包括演進型行動性管理(EMM)單元 665 和安全連線(SC)單元 370。SC 單元 370 包括 PD 單元 375。MM 單元 615 和 EPSBM 單元 605 介面兩者都具有 LTE AS 子層 620，該 LTE AS 子層 620 包括 RRC 680 和 PDCP 685。

EPS 承載實體 625、630 和 635 在 WTRU 與封包資料節點（PDN）閘道之間運行，並由無線電承載（RB）和 EPS 存取承載的組合組成。EPSBM 單元 605 控制 EPS 承載的改

變和配置。LTE AS 子層 620 提供服務給 MM 單元 615 和 EPSBM 單元 605。ESM 單元 645 提供服務給 EPSBM 單元 605，並使用 MM 單元 615 的服務。除了使用來自 EMM 單元 665 的服務之外，ESMS 實體 650 與用於 GSM 中的 GPRS 服務的 SMS 實體相同。除了使用來自 PS 發信連接的服務之外，SS 實體 655 與用於非 GPRS 的服務的一方相同。

SC 單元 670 被使用以使得來自 EMM 單元 665 和 ESM 單元 645 的所有訊息通過 SC 單元 670 被傳遞到 LTE AS 子層 620。如第 6 圖所示，SC 單元 670 可以被視為 MM 單元 615 的子實體，或者它可以被視為與 MM 單元 615 分離的 L3 實體。SC 單元 670 的功能性也可以駐留在較低層中（例如 RRC 680），並且它還可以被定義為具有其自身的協議。

就其功能來說，下面的任意組合可以被實現：

1）EMM、ESM 和其他實體（例如 SMS）可以發送訊息到 SC 單元 670。

2）可以定義 SAP 和相關聯的原語以用於 EMM 單元 665 和 SC 單元 670、以及 ESM 單元 645 和 SC 單元 670。

3）SC 單元 670（或者更一般地 NAS）可以定義 NAS 安全性狀態變數（例如 1 位元），該 NAS 安全性狀態變數指出當前的 NAS 安全性是否處於活動狀態。可能具有兩個這樣的變數以在加密與完整性保護之間進行區別。注意原語可以在 NAS 與 RRC 之間交換以指示加密的存在或不存在，而不是 1 位元 NAS 安全性狀態變數。同樣這一位元也可以被認為是分離的 PDU，該分離的 PDU 被用於指示加密

已經開始（例如分離的 NAS 訊息可以被用於這一目的）。可替換地，這一位元可以被包括在每個 NAS PDU 中。

4）SC 單元 670 可以在透明模式或非透明模式中操作。在透明模式中，SC 單元 670 將不對特定的 NAS 訊息進行加密/解密及/或完整性檢查。這一決定可以基於下面因素中的任意組合：訊息的協定鑒別符、L3 協議標頭中的指示符欄位（指示用於特定 PDU 的加密及/或完整性保護的需要）、訊息類型、NAS 安全性狀態變數、根據上層協定的指示（例如來自 EMM 單元 665 及/或 ESM 單元 645 到 SC 單元 670 的不對所述訊息進行加密/完整性檢查的指示）。

5）在非透明模式中，SC 單元 670 可以對相關的 NAS PDU 進行加密/解密及/或完整性檢查。這一決定也可以基於下面因素的任意組合：訊息的協定鑒別符、L3 協議標頭中的指示符欄位（指示用於特定 PDU 的加密及/或完整性保護的需要）、訊息類型、NAS 安全性狀態變數、根據上層協定的指示（例如來自 EMM 單元 665 及/或 ESM 單元 645 到 SC 單元 670 的不對所述訊息進行加密/完整性檢查的指示）。

6）在接收側，SC 單元 670 可以從較低層接收 NAS PDU，並且如果在透明模式中操作，則基於所述訊息的協定鑒別符將所述訊息路由到正確的上層實體（例如 EMM/ESM）。如果接收 SC 單元 670 在非透明模式中進行，則它可以對 NAS PDU 進行加密及/或完整性檢查、增加其 NAS SN 及/或 NAS HFN，然後基於 NAS 標頭的 PD 欄位路由所述訊息。接收側可以解密然後檢查訊息的完整性，或

反之亦然由傳輸側中的這些操作的順序決定。

如上所描述，可能可以具有用於SC單元670的分離的協定。這一協議可以藉由具有在L3標頭中的其自身的協議鑒別符欄位而被區別。屬於這一協定的訊息類型可以是涉及加密、認證、識別和與其他之間的密鑰協定。實例包括：

1）身份請求；

2）身份回應；

3）認證請求；

4）認證回應；

5）認證失敗；

6）認證拒絕；

7）NAS安全性模式指令；

8）NAS安全性模式指令完成；以及

9）NAS安全性模式指令失敗。

也可能可以定義用於這一實體的狀態機。例如，下面描述可能的狀態（可能可以應用其他用於這些狀態和其他狀態的名稱）：

a）SECURITY INACTIVE（安全性無效）：在這一狀態中，不向網路認證WTRU並且在WTRU或網路中不存在安全性上下文。作為這一狀態（或分離狀態）的子狀態，一方可以具有指出正在進行的AKA議程、NAS安全性模式指令交換以及RRC安全性模式指令交換的狀態。

b）SECURITY ACTIVE（安全性有效）：在這一狀態中，向網路認證WTRU並且在WTRU或網路中存在安全性上

下文。WTRU 可以具有某些密鑰（例如 K_{asme}）或所有密鑰。

可能還可以用雖然更複雜但不同的方式來實現這一相同的 SCE。例如，在傳輸側，具有構建的 NAS PDU 的上層傳呼實體（例如 EMM 單元 665 或 ESM 單元 645），可以將該構建的 NAS PDU 發送到 NAS SC 單元 670。然後 NAS SC 單元 670 可以對 PDU 進行加密及/或完整性檢查，然後將其返回到傳呼實體。然後傳呼實體可以將所保護的 NAS PDU 發送到更低層（即 RRC）。這一方法具有重新使用 MM 單元 615 與 LTE AS 子層 620 之間存在的 SAP 的優點。然而在接收側，在可以將訊息路由到正確的上層協定之前，對訊息進行解密和完整性檢查。這一功能可以藉由將所有接收到的 NAS PDU 路由到 SC 單元 670 來實現，然後 SC 單元 670 做出路由決定。

另一個選項是每個 NAS 層在其自身的協定中進行訊息的加密/完整性保護。從而 EMM 單元 665 可以對 EMM 訊息進行加密/完整性檢查/解密，並且 ESM 單元 645 可以對 ESM 訊息進行加密/完整性檢查/解密等。在這種情況中 SC 單元 670 的作用可以被限於提供序列號給 EMM 和 ESM 層（以及任意其他層），以使得正在使用的 SN 沒有衝突。這一問題可以藉由在每個協議 PDU 基礎上，而不是在每個 NAS PDU 基礎上定義要增加的 SN 而消失。在這種情況中，每個 NAS 子層（例如 EMM/ESM）可以具有其自身的 SN/HFN，該 SN/SFN 被增加以用於屬於這一協議的每個 NAS PDU。在這一方案中，在接收側，NAS 層中的路由實

體可以基於NAS標頭（假設它不被加密）中的協議鑒別符欄位將接收到的NAS PDU路由到正確的NAS實體，然後各自的協定實體可以對訊息進行解密及/或完整性檢查。

NAS PDU的長度的確定

NAS層可以將NAS PDU（待解密的）的部分的長度提供到加密引擎。以下是用於確定這一長度的不同選項。

1）傳送NAS實體可以包括在L3訊息（例如協定標頭中）中的長度的指示。這一長度可以是完整訊息、訊息的加密部分或允許接收NAS實體以確定需要產生的密鑰串流區塊的長度的一些其他值的長度。

2）傳送NAS實體可以包括當它傳遞用於傳輸的L3訊息時對到RRC的L3訊息的長度的指示。這一長度指示由接收器中的RRC層接收，並被傳遞到接收器NAS實體，這一長度指示被用於確定待產生的密鑰串流區塊的長度。

3）當前，NAS層期望完成NAS PDU而無需在NAS層執行重新分段。結果，當接收到NAS PDU時，接收實體可以確信它是完整的（如果它接收到丟失了期望值的訊息，它的行為是當前地丟棄訊息）。因而，可能留下NAS PDU的長度的確定一直到實現。

以下給出接收器中的一個示例實現：

1）接收到NAS PDU；

2）NAS PDU被存儲在記憶體/緩衝器或等價物中；

3）確定訊息的大小（例如被佔據的記憶體/緩衝器空間）；

4）藉由從訊息的大小中減去訊息的未加密部分的長度來確定訊息的加密部分的長度。訊息的未加密部分的長度可以是固定的或可以由已知模式變化（例如由訊息類型/協定決定）或者可以由接收 NAS 實體中的傳輸 NAS 實體配置；以及

5）加密部分的長度被傳遞到加密演算法以確定要用於解密的密鑰串流。

無線電鏈結失敗和切換後 NAS SN 和 HFN 的處理

作為這些過程的一部分，有必要確定當前 NAS SN 和 HFN 編號如何在網路中被處理。

在切換過程中，下面任意一項可以用當前在 WTRU 和源 MME 中的 NAS SN 和 HFN 來執行。

1）NAS HFN 和 NAS SN 兩者都可以被重設定為默認值。

2）NAS HFN 可以不被重設定但是 NAS SN 可以被重設定。NAS HFN 由源 MME 傳遞到目標以作為切換（HO）請求的一部分。

3）NAS SN 可以不被重設定，但 NAS HFN 可以被重設定。NAS SN 由源 MME 傳遞到目標以作為 HO 請求的一部分。

4）NAS HFN 和 NAS SN 兩者都可以不被重設定。它們都由源 MME 傳遞到目標以作為 HO 請求的一部分。

其他需要回答的問題是參數（NAS SN 及/或 HFN）中的任意一個是否都被重設定，此重設定何時被觸發以及新

的 NAS/ASME 密鑰如何被傳遞到 WTRU。

因此，在 MME 間切換過程中，NAS 訊息被從源 MME 觸發到 WTRU，以提供用於導出新的 NAS 和 ASME 密鑰的必要的參數。可替換地，源 MME 可以以安全的方式（使用現有的加密/完整性保護）提供具有新的 NAS 和 ASME 密鑰的 WTRU。例如，這一訊息可以是 NAS 安全性模式指令/重配置。這一 NAS 訊息可以先於切換指令（例如在分離的下鏈直接傳遞訊息中）、或者作為切換指令中的 L3 訊息而被發送。作為另一替換實施方式，該資訊可以在 RRC 訊息中直接被發送。

NAS SN 及/或 HFN 的重設定可以由切換臨近（例如當 RRC 接收切換指令時）的較低層指示來觸發，或者由所述分離的 NAS 訊息的接收來觸發。

無線電鏈結失敗和 e 節點-B 間切換後 NAS SN 和 HFN 的處理

由於上鏈（UL）和下鏈（DL）中的無線電鏈結（RL）失敗和 e 節點-B 間切換，NAS SN 及/或 HFN 可以被重設定。這可以由訊息（例如 RRC 訊息）的傳輸和接收來觸發。

在 NAS 處的重傳處理

在重傳的情況中，NAS 層可以檢測再次被傳送的封包是重複的 PDU（已接收到的 PDU）還是新的 PDU。重複檢測實體可以是位於 EMM 或 ESM 之下、並監控所引入的封包是否之前已被發送的通用實體。在未接收到用於傳送的 NAS PDU 的應答的事件中，較低層可以向 NAS 層提供這

一事件的指示。NAS 層可以使用這一指示以重新傳送具有相同 SN 的 PDU（或發送新的 PDU）。

在不允許重複檢測的情況中，與以新的序列號傳送資料相反，相同的序列號可以被用於傳送失敗的傳輸情況中的資料。

可替換地或另外，NAS 交易辨識符可以由 NAS 用以檢測重複訊息。這可能需要 NAS 事務 ID 作為 NAS 標頭的一部分。因而，WTRU 能夠讀取這一 ID 並丟棄接收到的任意重複訊息。

實施例

1．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息的標頭中的指示符欄位來確定是否加密所述 NAS 訊息。

2．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息的協定鑒別符（PD）來確定是否加密所述 NAS 訊息。

3．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息的類型來確定是否加密所述 NAS

訊息。

4．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於 NAS 安全性狀態變數來確定是否加密所述 NAS 訊息。

5．根據實施例 4 所述的方法，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

6．根據實施例 4 所述的方法，其中所述 NAS 安全性狀態變數包含一個位元。

7．根據實施例 4 所述的方法，其中所述 NAS 安全性狀態變數包含用於指示加密已經開始的 NAS 協定資料單元（PDU）。

8．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

基於根據無線電資源控制（RRC）協議的指示來確定是否加密所述 NAS 訊息。

9．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息的標頭中的指示符欄位來確定是否對所述 NAS 訊息執行完整性檢查。

10．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息的協定鑒別符（PD）來確定是否執行完整性檢查。

11．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息的類型來確定是否對所述 NAS 訊息執行完整性檢查。

12．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於 NAS 安全性狀態變數來確定是否對所述 NAS 訊息執行完整性檢查。

13．根據實施例 12 所述的方法，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

14．根據實施例 13 所述的方法，其中所述 NAS 安全性狀態變數包含一個位元。

15．根據實施例 13 所述的方法，其中所述 NAS 安全性狀態變數包含用於指示加密已經開始的 NAS 協定資料單元（PDU）。

16．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於根據無線電資源控制（RRC）協議的指示來確定

是否執行完整性檢查。

17．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

從較低層接收NAS協定資料單元(PDU)，該NAS PDU包含協定鑒別符（PD）欄位；

加密所述NAS PDU；

增量NAS序列號（SN）和與所述NAS PDU關聯的超訊框號（HFN）中的至少其中之一；以及

基於所述PD欄位而將所述NAS PDU路由至上層實體。

18．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

從較低層接收NAS協定資料單元(PDU)，該NAS PDU包含協定鑒別符（PD）欄位；

對所述NAS PDU執行完整性檢查；

增量NAS序列號（SN）和與所述NAS PDU關聯的超訊框號（HFN）中的至少其中之一；以及

基於所述PD欄位而將所述NAS PDU路由至上層實體。

19．一種無線傳輸/接收單元（WTRU），該WTRU包括：

演進型會話管理（ESM）單元，被配置以產生非存取層（NAS）訊息；以及

安全連線（SC）單元，被配置以基於所述NAS訊息的

協定鑒別符（PD）、所述 NAS 訊息的標頭中的指示符欄位元、所述 NAS 訊息的類型、NAS 安全性狀態變數以及根據無線電資源控制（RRC）協議的指示中的至少其中之一來確定是否加密所述 NAS 訊息。

20．根據實施例 19 所述的 WTRU，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

21．根據實施例 20 所述的 WTRU，其中所述 NAS 安全性狀態變數包含一個位元。

22．根據實施例 20 所述的 WTRU，其中所述 NAS 安全性狀態變數包含用於指示加密已經開始的 NAS 協定資料單元（PDU）。

23．根據實施例 19 所述的 WTRU，其中所述 SC 單元包含 PD 單元。

24．一種無線傳輸/接收單元（WTRU），該 WTRU 包括：

演進型會話管理（ESM）單元，被配置以產生非存取層（NAS）訊息；以及

安全連線（SC）單元，被配置以基於所述 NAS 訊息的協定鑒別符（PD）、所述 NAS 訊息的標頭中的指示符欄位元、所述 NAS 訊息的類型、NAS 安全性狀態變數以及根據無線電資源控制（RRC）協議的指示中的至少其中之一來確定是否解密所述 NAS 訊息。

25．根據實施例 24 所述的 WTRU，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

26．根據實施例 25 所述的 WTRU，其中所述 NAS 安全性狀態變數包含一個位元。

27．根據實施例 25 所述的 WTRU，其中所述 SC 單元包含 PD 單元。

28．一種無線傳輸/接收單元（WTRU），該 WTRU 包括：

演進型會話管理（ESM）單元，被配置以產生非存取層（NAS）訊息；以及

安全連線（SC）單元，被配置以基於所述 NAS 訊息的協定鑒別符（PD）、所述 NAS 訊息的標頭中的指示符欄位元、所述 NAS 訊息的類型、NAS 安全性狀態變數以及根據無線電資源控制（RRC）協議的指示中的至少其中之一來確定是否對所述 NAS 訊息執行完整性檢查。

29．根據實施例 28 所述的 WTRU，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

30．根據實施例 29 所述的 WTRU，其中所述 NAS 安全性狀態變數包含一個位元。

31．根據實施例 28 所述的 WTRU，其中所述 SC 單元包含 PD 單元。

32．一種無線傳輸/接收單元（WTRU），該 WTRU 包括：

演進型移動性管理（EMM）單元，被配置以產生非存取層（NAS）訊息；以及

安全連線（SC）單元，被配置以基於所述 NAS 訊息的

協定鑒別符（PD）、所述 NAS 訊息的標頭中的指示符欄位元、所述 NAS 訊息的類型、NAS 安全性狀態變數以及根據無線電資源控制（RRC）協議的指示中的至少其中之一來確定是否加密所述 NAS 訊息。

33．根據實施例 32 所述的 WTRU，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

34．根據實施例 33 所述的 WTRU，其中所述 NAS 安全性狀態變數包含一個位元。

35．根據實施例 33 所述的 WTRU，其中所述 NAS 安全性狀態變數包含用於指示加密已經開始的 NAS 協定資料單元（PDU）。

36．根據實施例 32 所述的 WTRU，其中所述 SC 單元包含 PD 單元。

37．一種無線傳輸/接收單元（WTRU），該 WTRU 包括：

演進型移動性管理（EMM）單元，被配置以產生非存取層（NAS）訊息；以及

安全連線（SC）單元，被配置以基於所述 NAS 訊息的協定鑒別符（PD）、所述 NAS 訊息的標頭中的指示符欄位元、所述 NAS 訊息的類型、NAS 安全性狀態變數以及根據無線電資源控制（RRC）協議的指示中的至少其中之一來確定是否對所述 NAS 訊息執行完整性檢查。

38．根據實施例 37 所述的 WTRU，其中所述 NAS 安全性狀態變數用於指示 NAS 安全性當前是否被啟動。

39．根據實施例 38 所述的 WTRU，其中所述 NAS 安全性狀態變數包含一個位元。

40．根據實施例 37 所述的 WTRU，其中所述 SC 單元包含 PD 單元。

41．一種在無線傳輸/接收單元（WTRU）中處理非存取層（NAS）訊息的方法，該方法包括：

生成 NAS 訊息；以及

基於所述 NAS 訊息中的指示來確定需要產生的密鑰串流區塊的長度。

42．根據實施例 41 所述的方法，其中所述指示傳達了所述 NAS 訊息的整個長度。

43．根據實施例 41 所述的方法，其中所述指示傳達了允許接收 NAS 實體確定要產生的密鑰串流區塊的長度的值。

44．一種無線傳輸/接收單元（WTRU），該 WTRU 包括：

演進型移動性管理（EMM）單元，被配置以產生非存取層（NAS）訊息；以及

安全連線（SC）單元，被配置以基於所述 NAS 訊息中的指示來確定需要產生的密鑰串流區塊的長度。

45．根據實施例 44 所述的 WTRU，其中所述指示傳達了所述 NAS 訊息的整個長度。

46．根據實施例 44 所述的 WTRU，其中所述指示傳達了允許接收 NAS 實體確定要產生的密鑰串流區塊的長度的

值。

雖然本發明的特徵和元素以特定的結合進行了描述，但每個特徵或元素可以在沒有其他特徵和元素的情況下單獨使用，或在與或不與其他特徵和元素結合的各種情況下使用。這裏提供的方法或流程圖可以在由通用電腦或處理器執行的電腦程式、軟體或韌體中實施。關於電腦可讀存儲介質的實例包括唯讀記憶體（ROM）、隨機存取記憶體（RAM）、寄存器、緩衝記憶體、半導體存儲設備、內部硬碟和可行動磁片之類的磁介質、磁光介質以及 CD-ROM 磁片和數位多功能光碟（DVD）之類的光介質。

舉例來說，恰當的處理器包括：通用處理器、專用處理器、常規處理器、數位信號處理器（DSP）、多個微處理器、與 DSP 核相關聯的一個或多個微處理器、控制器、微控制器、專用積體電路（ASIC）、現場可編程閘陣列（FPGA）電路、任何一種積體電路（IC）及/或狀態機。

與軟體相關聯的處理器可以用於實現一個射頻收發器，以便在無線傳輸接收單元（WTRU）、使用者設備（UE）、終端、基地台、無線網路控制器（RNC）或任何主機電腦中加以使用。WTRU 可以與採用硬體及/或軟體形式實施的模組結合使用，例如相機、攝像機模組、視訊電話、揚聲器電話、振動設備、揚聲器、麥克風、電視收發機、免持耳機、鍵盤、藍牙®模組、調頻（FM）無線單元、液晶顯示器（LCD）顯示單元、有機發光二極體（OLED）顯示單元、數位音樂播放器、媒體播放器、視頻遊戲機模組、網

際網路流覽器及/或任何無線局域網（WLAN）或超寬頻（UWB）模組。

【圖式簡單說明】

從以下描述中可以更詳細地理解本發明，這些描述是以實例結合附圖的方式給出的，其中：

第 1 圖示出了常規 LTE L3 標頭的結構；

第 2 圖示出了第 1 圖的 LTE L3 標頭的 PD 欄位；

第 3 圖示出了僅 PS 的 UMTS WTRU 的常規 NAS 架構；

第 4 圖示出了 NAS 訊息 IE 的類型/長度/數值（TLV）編碼的格式；

第 5 圖示出了常規 MME 間切換過程的一個實例；

第 6 圖示出了新的 NAS 架構的一個實例。

【主要元件符號說明】

100	長期演進層三標頭
105	交易辨識符或跳躍指示符欄位
110	協議鑒別符
115	第二個八位元組包括訊息類型欄位
120	其他需要的資訊元素
300	非存取層架構
305	無線電存取承載管理單元
310	連接管理單元
315	行動性管理單元
320	存取層子層
325、330、335	無線電存取承載實體
340	無線電存取承載控制單元

345	議程管理單元
350	通用封包無線電服務短訊息服務實體
355	補充服務實體
360	封包資料協定
365	通用封包無線電服務行動性管理單元
370	協議鑒別符
375	無線電資源控制器
380	廣播多播控制器
385	封包資料彙聚協定
600	非存取層層 3 架構
605	演進型封包系統承載管理單元
610	連接管理單元
615	移動性管理單元
620	長期演進存取層子層
625	演進型封包系統承載實體 1
630	演進型封包系統承載實體 2
635	演進型封包系統承載實體 3
640	演進型封包系統承載控制單元
645	演進型議程管理單元
650	演進型短訊息服務實體
655	補充服務實體
660、PDP	封包資料協定
665	演進型行動性管理單元
670	安全連線單元

675	協議鑒別符單元
680	無線電資源控制
685	封包資料彙聚協定
T	類型
V	數值
TV	類型和數值
LV	長度和數值
TLV	類型、長度和數值
WTRU	無線傳輸/接收單元
MME	行動性管理實體
HO	切換
NAS	非存取層
EPS	演進型封包系統
ESMS	演進型短訊息服務
SS	補充服務
LTE	長期演進
RRC	無線電資源控制
PDCP	封包資料彙聚協定
PDP	封包資料協定
TI	交易辨識符

七、申請專利範圍：

1. 一種在一無線傳輸/接收單元（WTRU）中處理複數個非存取層（NAS）訊息的方法，該方法包括：

生成一 NAS 訊息以及包括一 NAS 安全性狀態變數的一 NAS 標頭；

基於所述NAS安全性狀態變數來確定是否加密所述NAS 訊息，其中所述 NAS 安全性狀態變數在其具有一第一值時指示出 NAS 安全性當前對於所述 NAS 訊息是啟動的並且在所述NAS安全性狀態變數具有一第二值時指示出 NAS 安全性當前對於所述 NAS 訊息是不啟動的；以及

基於所述NAS 標頭的一協定鑒別符（PD）欄位來路由所述 NAS 訊息。

2. 如申請專利範圍第 1 項所述的方法，其中所述 NAS 安全性狀態變數包含一位元。

3. 如申請專利範圍第 1 項所述的方法，其中所述 NAS 訊息是一長期演進（LTE）演進型移動性管理（EMM）訊息或一 LTE 演進型會話管理（ESM）訊息。

4. 如申請專利範圍第 1 項所述的方法，其中所述 NAS 訊息包括一 NAS 協定資料單元（PDU）。

5. 如申請專利範圍第 4 項所述的方法，其中一編碼的 NAS PDU 指出所述加密步驟目前是啟動的。

6. 如申請專利範圍第 1 項所述的方法，其中所述 PD 值是專用於 EMM 或 ESM NAS 訊息。

7．一種無線傳輸/接收單元（WTRU），該 WTRU 包括：

一處理器，被配置用於生成一非存取層（NAS）訊息以及包括一 NAS 安全性狀態變數的一 NAS 標頭；

該處理器更被配置用於基於所述 NAS 安全性狀態變數來確定是否加密所述 NAS 訊息，其中在所述 NAS 安全性狀態變數具有一第一值的情況下，NAS 安全性對於所述 NAS 訊息是啟動的，並且在所述 NAS 安全性狀態變數具有一第二值的情況下，NAS 安全性對於所述 NAS 訊息是不啟動的；以及

一處理器，更被配置用於基於所述 NAS 標頭的一協定鑒別符（PD）欄位來路由所述 NAS 訊息。

8．如申請專利範圍第 7 項所述的無線傳輸/接收單元（WTRU），其中所述 NAS 訊息是一長期演進（LTE）演進型移動性管理（EMM）訊息或一 LTE 演進型會話管理（ESM）訊息。

9．如申請專利範圍第 7 項所述的無線傳輸/接收單元（WTRU），其中所述 NAS 訊息包括一 NAS 協定資料單元（PDU）。

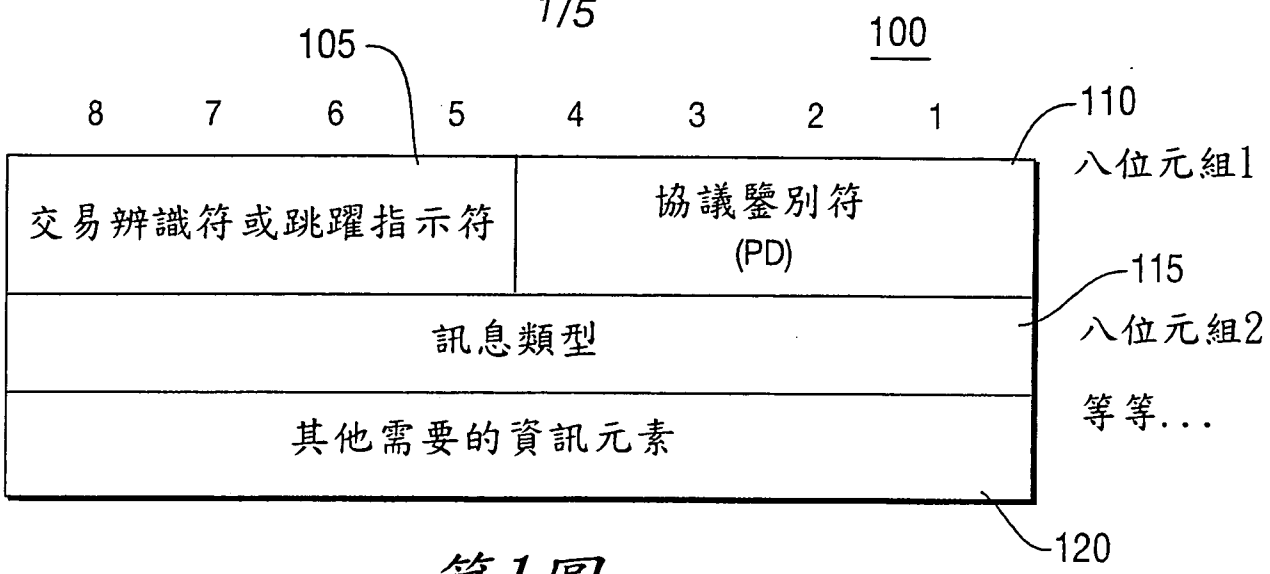
10．如申請專利範圍第 9 項所述的無線傳輸/接收單元（WTRU），其中一編碼的 NAS PDU 指出所述加密步驟目前是啟動的。

11．如申請專利範圍第 7 項所述的無線傳輸/接收單元（WTRU），其中所述 NAS 安全性狀態變數包含一位元。

12．如申請專利範圍第 7 項所述的無線傳輸/接收單元

（WTRU），其中所述 PD 值是專用於 EMM 或 ESM NAS 訊息。

八、圖式：

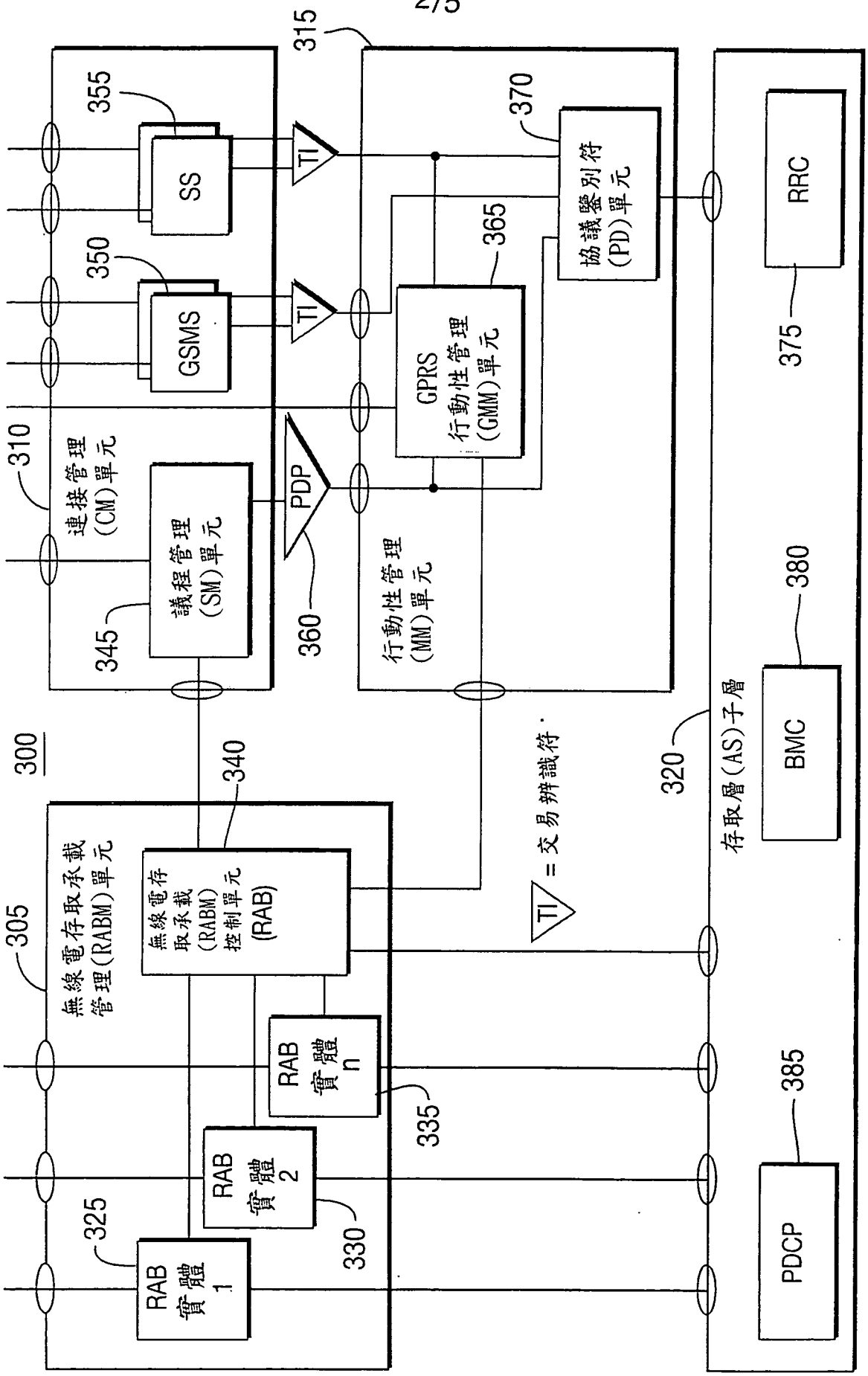


第1圖

110

位元 4321	
0000	分組傳呼控制
0001	廣播傳呼控制
0010	保留:在協議的較早階段中被分配
0011	傳呼控制:傳呼相關的SS消息
0100	GPRS透明傳輸協議(GTTP)
0101	行動性管理訊息
0110	無線電資源管理訊息
1000	GPRS移動性管理訊息
1001	SMS訊息
1010	GPRS議程管理訊息
1011	非傳呼相關的SS訊息
1100	定位服務
1110	擴展到一個八位元組長度的PD的擴展的保留
1111	測試過程的保留

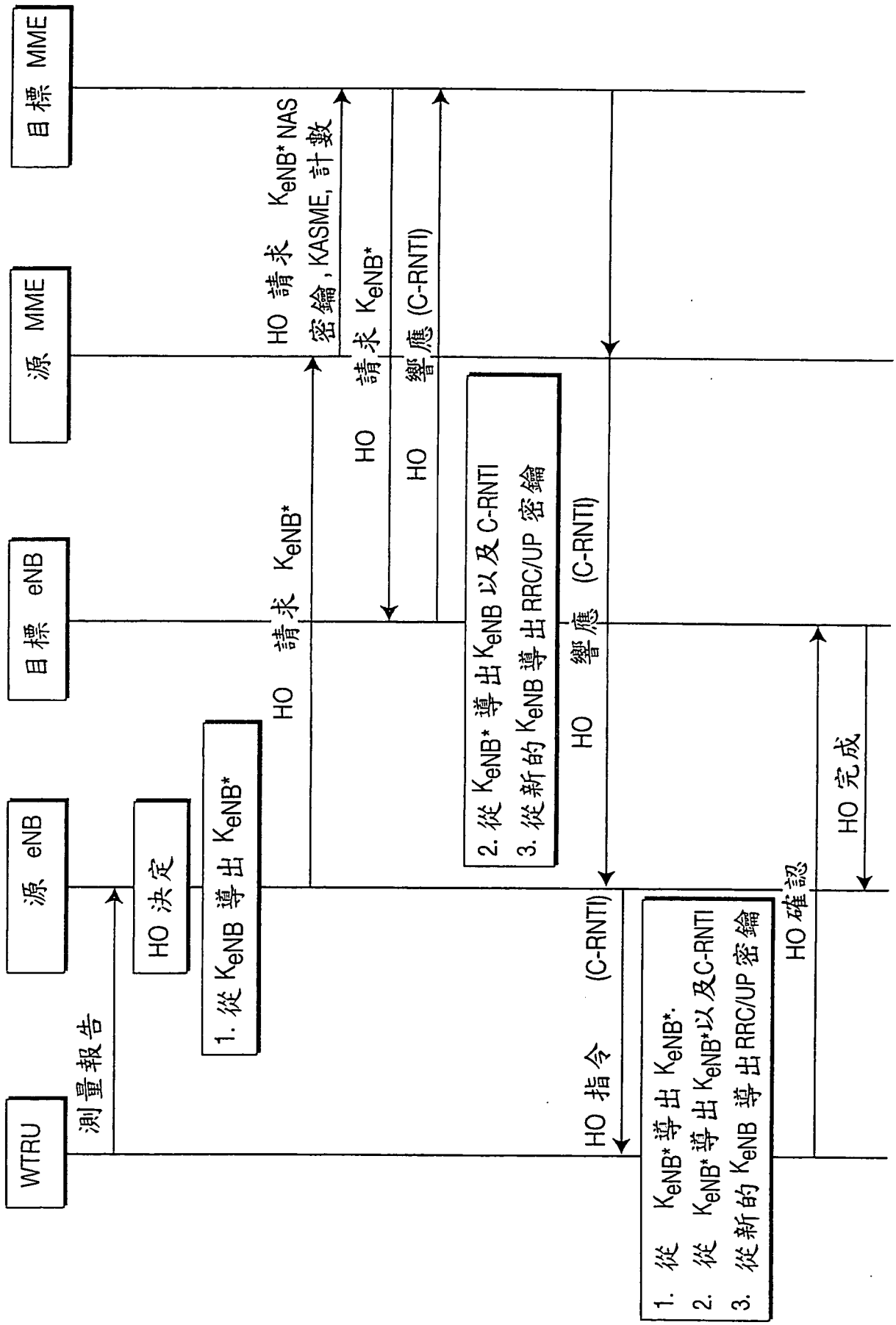
第2圖


300
305
無線電存取承載管理(RABM)單元
310
連接管理(CM)單元
315
320
存取層(AS)子層
325
RAB實體1
330
RAB實體2
335
RAB實體n
340
無線電存取承載(RABM)控制單元(RAB)
345
議程管理(SM)單元
350
GSMS
355
SS
360
PDP
365
GPRS行動性管理(GMM)單元
370
協議鑒別符(PD)單元
375
RRC
380
BMC
385
PDCP
行動性管理(MM)單元
TI
TI
TI
= 交易辨識符
= 服務存取點(SAP)

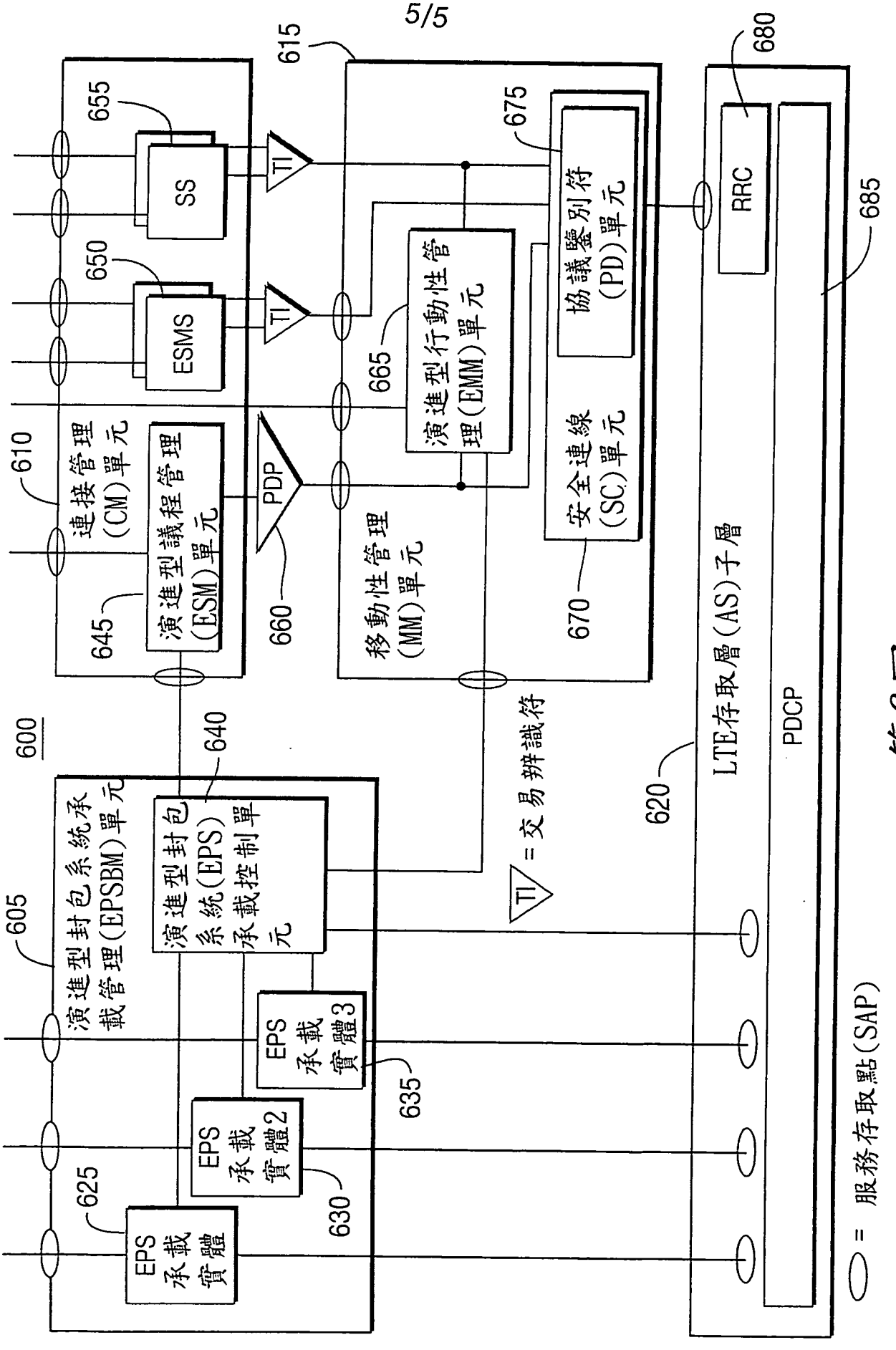
第3圖

	格式	含義	IP指示符(類型)存在	長度指示符存在	數值指示符存在
405	T	僅類型	是	否	否
410	V	僅數值	否	否	是
415	TV	類型和數值	是	否	是
420	LV	長度和數值	否	是	是
425	TLV	類型、長度和數值	是	是	是

第4圖


WTRU
源 eNB
目標 eNB
源 MME
目標 MME
測量報告
HO 決定
1. 從 KeNB 導出 KeNB*
HO 請求 KeNB*
HO 請求 KeNB* NAS 密鑰, KASME, 計數
HO 請求 KeNB*
HO 響應 (C-RNTI)
2. 從 KeNB* 導出 KeNB 以及 C-RNTI
3. 從新的 KeNB 導出 RRC/UP 密鑰
HO 響應 (C-RNTI)
HO 指令 (C-RNTI)
1. 從 KeNB* 導出 KeNB*.
2. 從 KeNB* 導出 KeNB* 以及C-RNTI
3. 從新的 KeNB 導出 RRC/UP 密鑰
HO 確認
HO 完成

第5圖


600
605
演進型封包系統承載管理(EPSBM)單元
610
連接管理(CM)單元
615
620
LTE存取層(AS)子層
625
EPS承載實體
630
EPS承載實體2
635
EPS承載實體3
640
演進型封包系統(EPS)承載控制單元
645
演進型議程管理(ESM)單元
650
ESMS
655
SS
660
PDP
665
演進型行動性管理(EMM)單元
670
安全連線(SC)單元
675
協議鑒別符(PD)單元
680
RRC
685
PDCP
移動性管理(MM)單元
TI = 交易辨識符
= 服務存取點(SAP)

第6圖