



(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 I713614 B

(45)公告日：中華民國 109 (2020) 年 12 月 21 日

(21)申請案號：105134715

(22)申請日：中華民國 105 (2016) 年 10 月 27 日

(51)Int. Cl. : **H04W88/06 (2009.01)****H04L12/70 (2013.01)**

(30)優先權：2015/11/17 美國

62/256,472

2016/02/19 美國

15/048,044

(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)；法西 史帝法諾 FACCIN, STEFANO (US)；霍恩

蓋文伯納德 HORN, GAVIN BERNARD (US)；納希斯基 約翰 NASIELSKI,

JOHN (US)；千波寧瑞 雷納吉納維夫 CHAPONNIERE, LENAIG GENEVIEVE

(US)

(74)代理人：李世章

(56)參考文獻：

TW 201507400A

US 2013/0080782A1

US 2014/0064209A1

US 2014/0119353A1

US 2015/0229620A1

WO 2011/043772A1

審查人員：林東威

申請專利範圍項數：28 項 圖式數：23 共 93 頁

(54)名稱

用於使用支援多個連線性和服務上下文的安全模型的無線通訊的方法和裝置

(57)摘要

本案內容的態樣提供了用於在共享單個連線性上下文時實現多個連線性和服務上下文以建立網路連接的安全模型。上下文（例如，連線性上下文、服務上下文、安全性上下文）是描述在兩個或兩個以上實體之間建立的連線性、服務或安全性的資訊集合。連線性上下文和服務上下文可以在不同的網路節點或實體處建立。在本案內容的一個態樣中，連線性上下文包括進化型封包系統（EPS）行動性管理（EMM）上下文或者 EMM 上下文和 EPS 通信期管理（ESM）上下文二者。

Aspects of the present disclosure provide for a security model for enabling multiple connectivity and service contexts while sharing a single connectivity context to establish a network connection. A context (e.g., connectivity context, service context, security context) is a set of information describing the connectivity, service, or security established between two or more entities. The connectivity context and service context may be established at different network nodes or entities. In one aspect of the disclosure, a connectivity context includes an Evolved Packet System (EPS) Mobility Management (EMM) context or both an EMM context and an EPS Session Management (ESM) context.

指定代表圖：

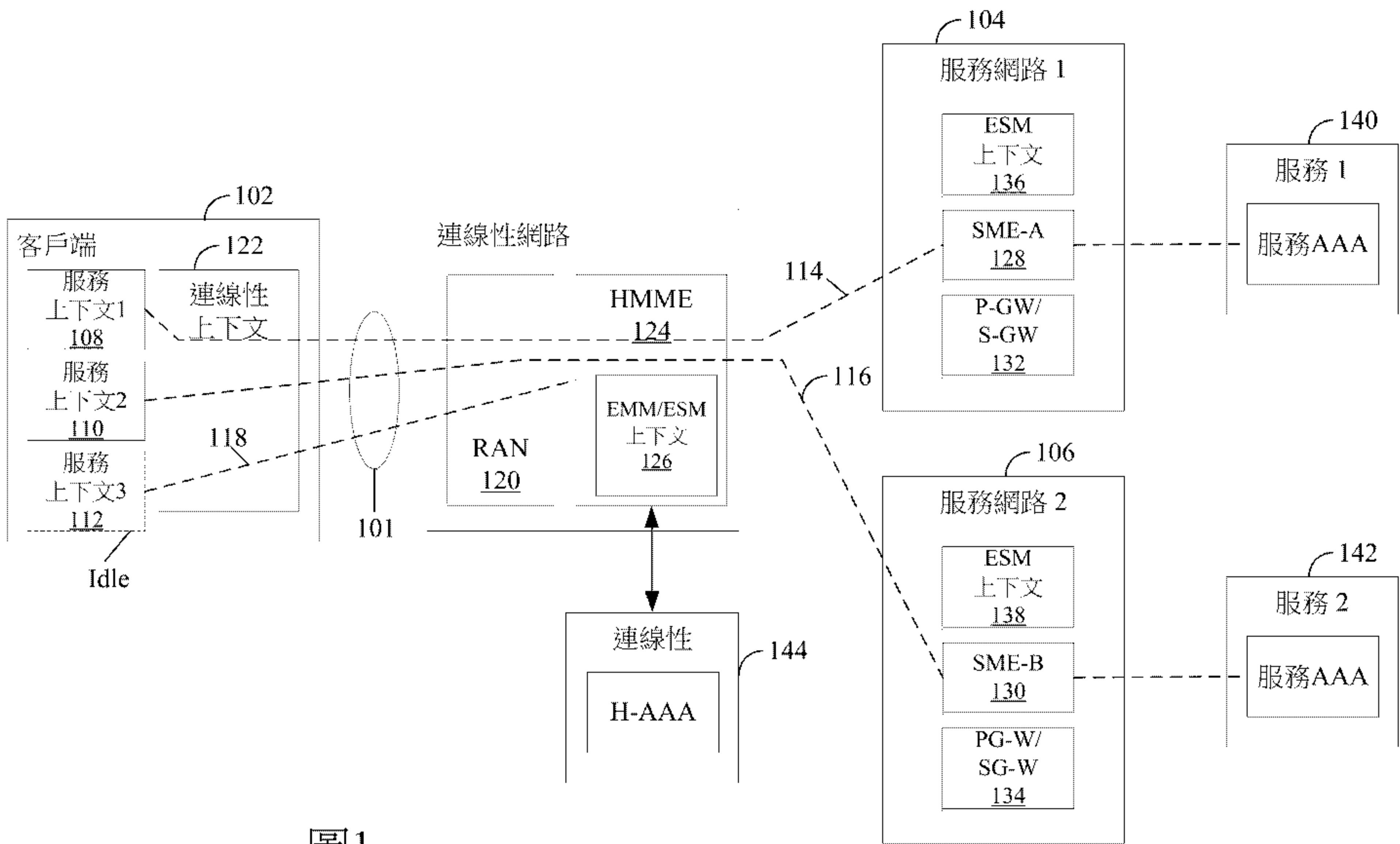


圖1

符號簡單說明：

- 101 . . . 無線電鏈路
- 102 . . . 客戶端設備
- 104 . . . 服務提供者
- 106 . . . 供應功能單元
- 108 . . . 服務上下文
- 110 . . . 服務上下文
- 112 . . . 服務上下文
- 114 . . . 服務連接
- 116 . . . 服務連接
- 118 . . . 服務連接
- 120 . . . RAN
- 122 . . . 連線性上下文
- 124 . . . 主 MME (HMME)
- 126 . . . EMM/ESM 上下文
- 128 . . . SME
- 130 . . . SME
- 132 . . . 服務閘道 (S-GW)
- 134 . . . 服務閘道 (S-GW)
- 136 . . . ESM 上下文
- 138 . . . ESM 上下文
- 140 . . . AAA 伺服器
- 142 . . . AAA 伺服器
- 144 . . . 歸屬授權、認證和計費(H-AAA) 伺服器



I713614

公告本

申請日: 105/10/27

IPC分類: *H04W 88/06* (2009.01)  
*H04L 12/70* (2013.01)

## 【發明摘要】

【中文發明名稱】用於使用支援多個連線性和服務上下文的安全模型的無線通訊的方法和裝置

【英文發明名稱】METHODS AND APPARATUS FOR WIRELESS COMMUNICATION USING A SECURITY MODEL TO SUPPORT MULTIPLE CONNECTIVITY AND SERVICE CONTEXTS

## 【中文】

本案內容的態樣提供了用於在共享單個連線性上下文時實現多個連線性和服務上下文以建立網路連接的安全模型。上下文（例如，連線性上下文、服務上下文、安全性上下文）是描述在兩個或兩個以上實體之間建立的連線性、服務或安全性的資訊集合。連線性上下文和服務上下文可以在不同的網路節點或實體處建立。在本案內容的一個態樣中，連線性上下文包括進化型封包系統（EPS）行動性管理（EMM）上下文或者EMM上下文和EPS通信期管理（ESM）上下文二者。

## 【英文】

Aspects of the present disclosure provide for a security model for enabling multiple connectivity and service contexts while sharing a single connectivity context to establish a network connection. A context (e.g., connectivity context, service context, security context) is a set of information describing the connectivity, service, or security established between two or more entities. The connectivity context and service context may be established at different network nodes or entities. In one aspect of the disclosure, a connectivity context includes an

申請案號：

申請日：

IPC 分類：

Evolved Packet System (EPS) Mobility Management (EMM) context or both an EMM context and an EPS Session Management (ESM) context.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

- 1 0 1 無 線 電 鏈 路
- 1 0 2 客 戶 端 設 備
- 1 0 4 服 務 提 供 者
- 1 0 6 供 應 功 能 單 元
- 1 0 8 服 務 上 下 文
- 1 1 0 服 務 上 下 文
- 1 1 2 服 務 上 下 文
- 1 1 4 服 務 連 接
- 1 1 6 服 務 連 接
- 1 1 8 服 務 連 接
- 1 2 0 R A N
- 1 2 2 連 線 性 上 下 文
- 1 2 4 主 M M E （ H M M E ）
- 1 2 6 E M M / E S M 上 下 文
- 1 2 8 S M E
- 1 3 0 S M E
- 1 3 2 服 務 閘 道 （ S - G W ）
- 1 3 4 服 務 閘 道 （ S - G W ）
- 1 3 6 E S M 上 下 文
- 1 3 8 E S M 上 下 文

申請案號：

申請日：

IPC 分類：

1 4 0    A A A 伺 服 器

1 4 2    A A A 伺 服 器

1 4 4    歸 屬 授 權 、 認 證 和 計 費 （ H - A A A ） 伺 服 器

【特徵化學式】

無

## 【發明說明書】

【中文發明名稱】用於使用支援多個連線性和服務上下文的安全模型的無線通訊的方法和裝置

【英文發明名稱】METHODS AND APPARATUS FOR WIRELESS COMMUNICATION USING A SECURITY MODEL TO SUPPORT MULTIPLE CONNECTIVITY AND SERVICE CONTEXTS

相關申請案的交叉引用

【0001】 本專利申請案主張享受於2015年11月17日在美國專利商標局遞交的臨時申請案第62/256,472號和於2016年2月19日在美國專利商標局遞交的非臨時申請案第15/048,044號的優先權和利益。

【技術領域】

【0002】 概括地說，下文論述的技術係關於無線通訊系統，並且更具體地係關於用於支援多個連線性和服務上下文的安全模型。

【先前技術】

【0003】 當前無線系統典型地工作在封包交換域中。無線系統的一些實例是LTE（長期進化）、LTE-A（改進的LTE）和WLAN（無線區域網路）。此類無線系統典型地經由在使用者設備與網路的連線性管理部分之間使用單個連線性上下文而僅支援單個訂閱及/或單個憑證。在LTE實例中，單個非存取層（NAS）上下文可以被使用在使用者裝置（UE）（使用者設備）與行動性管理實體（MME）之間。在LTE中，NAS是被用來在UE與MME

之間傳送用於LTE存取的非無線電相關的訊號傳遞的協定集合。連線性上下文一般代表與兩個實體（例如，使用者設備到網路實體或網路實體到網路實體）之間的連接相關聯的或定義該連接的資訊。

【0004】 在相關領域中，使用者設備（例如，行動設備或UE）一般包括用戶辨識模組（SIM）卡，該SIM卡包括對於該SIM卡唯一的標識資訊和金鑰。使用對由網路服務供應商提供的服務的訂閱的使用者設備能夠憑藉被儲存在該SIM卡上的標識和金鑰（或認證）資訊與該網路建立無線電鏈路或連線性。換句話說，在存取鏈路與連線性上下文的使用之間存在緊密的關係（例如，一對一的關係）。在蜂巢網路的情況下，存取鏈路的實例包括使用者平面和無線電資源控制（RRC）或媒體存取控制（MAC）訊號傳遞連接。在LTE實例中，建立無線電鏈路涉及EMM（進化型封包系統（EPS）行動性管理）上下文和ESM（EPS通信期管理）上下文。此外，在LTE實例中，當UE連接到網路時，在行動性管理實體（MME）處建立行動性管理上下文（EMM上下文）和通信期管理上下文（ESM上下文）。EMM上下文和ESM上下文二者與被儲存在SIM卡中的單個憑證（例如，SIM憑證）相關聯。該憑證允許MME決定該UE是否能夠被認證以建立所請求的連接。在該情況下，該MME向所有可用服務的一個提供者提供一個認證點。在該對上下文與SIM憑證之間存

在一對一的關聯。因此，可以說該對相關的上下文被緊密地耦合至該SIM憑證。

**【發明內容】**

**【0005】** 下面提出了對本案內容的一或多個態樣的簡要概述，以便提供對此類態樣的基本理解。該概述不是對本案內容的全部預期特徵的泛泛概括，並且既不意欲標識本案內容的全部態樣的關鍵的或決定性的元素亦不意欲圖示本案內容的任意或全部態樣的範疇。其唯一目的在於以簡化的形式提出本案內容的一或多個態樣的一些概念，作為稍後提出的更詳細的描述的序言。

**【0006】** 本案內容的態樣揭示一種用於支援多個連線性和服務上下文的安全模型。不同的憑證可以被用來建立連線性上下文和多個服務上下文。

**【0007】** 本案內容的一個態樣提供了一種在無線通訊網路中操作客戶端設備的方法。根據該方法，客戶端設備基於第一憑證來與連線性網路建立連接。客戶端設備建立與連接相對應的連線性上下文。客戶端設備辨識與連線性網路相關聯的一或多個服務網路。客戶端設備使用所建立的連接與一或多個服務網路建立一或多個服務連接，其中一或多個服務連接是使用各自的第二憑證建立的。客戶端設備建立分別與服務連接相對應的一或多個服務上下文。一或多個服務上下文分別包括不同的安全性上下文。安全性上下文之每一者安全性上下文包括非存取層

( N A S ) 安全性上下文和存取層 ( A S ) 安全性上下文，二者與相同的第二憑證相對應。

【 0 0 0 8 】 本案內容的一個態樣提供了一種操作連線性網路的網路節點的方法。根據該方法，網路節點基於連線性憑證來與客戶端設備建立第一連接。網路節點建立與第一連接相對應的連線性上下文。網路節點接收來自客戶端設備的針對與一或多個服務網路建立連接的請求。網路節點使用網路節點作為代理，為客戶端設備分別建立與服務網路的複數個第二連接。網路節點包括主行動性管理實體 ( H M M E ) 。

【 0 0 0 9 】 本案內容的一個態樣提供了一種操作服務網路的網路節點的方法。根據該方法，網路節點接收來自客戶端設備的針對建立連接的請求。網路節點經由連線性網路的網路節點來與客戶端設備建立連接。連線性網路的網路節點包括主行動性管理實體 ( H M M E ) 。網路節點建立與連接相對應的服務上下文，其中服務上下文與安全性上下文相關聯。

【 0 0 1 0 】 本案內容的一個態樣提供了一種無線通訊網路中的客戶端設備。客戶端設備包括被儲存有電腦可執行代碼的記憶體、被配置為與連線性網路通訊的通訊介面、以及被操作地耦合到記憶體和通訊介面的處理器。處理器被電腦可執行代碼配置為基於第一憑證與連線性網路建立連接。處理器亦被配置為建立與連接相對應的連線性上下文。處理器亦被配置為辨識與連線性網路相關聯的一或

多個服務網路。處理器亦被配置為使用所建立的連接來與一或多個服務網路建立一或多個服務連接。一或多個服務連接是使用各自的第二憑證建立的。處理器亦被配置為建立分別與服務連接相對應的一或多個服務上下文。一或多個服務上下文分別包括不同的安全性上下文。安全性上下文之每一者安全性上下文包括非存取層（NAS）安全性上下文和存取層（AS）安全性上下文，二者與相同的第二憑證相對應。

【0011】 本案內容的一個態樣提供了一種連線性網路的網路節點。網路節點包括被儲存有電腦可執行代碼的記憶體、被配置為與客戶端設備通訊的通訊介面、以及被操作地耦合到記憶體和通訊介面的處理器。處理器被電腦可執行代碼配置為基於連線性憑證來與客戶端設備建立第一連接。處理器亦被配置為建立與第一連接相對應的連線性上下文。處理器亦被配置為接收來自客戶端設備的針對與一或多個服務網路建立服務連接的請求。處理器亦被配置為使用網路節點作為代理，為客戶端設備分別建立與服務網路的複數個第二連接。網路節點包括主行動性管理實體（HME）。

【0012】 本案內容的一個態樣提供了一種服務網路的網路節點。網路節點包括被儲存有電腦可執行代碼的記憶體、被配置為與客戶端設備通訊的通訊介面、以及被操作地耦合到記憶體和通訊介面的處理器。處理器被可執行代碼配置為接收來自客戶端設備的針對建立連接的請求。處

理器亦被配置為經由連線性網路的網路節點來與客戶端設備建立連接。連線性網路的網路節點包括主行動性管理實體（H M M E）。處理器亦被配置為建立與連接相對應的服務上下文，其中服務上下文與安全性上下文相關聯。

【0013】 在審閱下面的具體實施方式時，將會更全面地理解本發明的這些和其他態樣。在結合附圖審閱下面的本發明的具體的、示例性的實施例的描述時，對於本發明所屬領域中具有通常知識者來說，本發明的其他態樣、特徵和實施例將變得顯而易見。儘管可以相對於下文的某些實施例和附圖來論述本發明的特徵，但是本發明的所有實施例可以包括本文論述的有利特性中的一或多個。換句話說，儘管可以將一或多個實施例論述為具有某些有利的特徵，但是此類特徵中的一或多個亦可以根據本文論述的本發明的各個實施例來使用。以類似的方式，儘管下文將示例性實施例論述為設備、系統或方法實施例，但是應當理解的是，此類示例性實施例可以被實現在各種設備、系統和方法中。

#### 【圖式簡單說明】

【0014】 圖1是根據本案內容的態樣圖示用於支援與不同的服務上下文相關聯的多個服務連接的客戶端設備與無線電存取網路（R A N）之間的單個無線電鏈路的示意圖。

【0015】圖2根據本案內容的態樣圖示被配置為使用單個無線電鏈路來支援多個同時的服務上下文的示例性客戶端設備。

【0016】圖3根據本案內容的態樣圖示用於實現主行動性管理實體（HMM E）及/或服務管理實體（SME）的示例性網路節點，其中HMM E及/或SME被配置為在單個無線電鏈路上操作時支援客戶端設備同時支援多個服務上下文的同時操作。

【0017】圖4是根據本案內容的態樣圖示HMM E控制平面模型的第一實例的示意圖。

【0018】圖5是根據本案內容的態樣圖示HMM E控制平面模型的第二實例的示意圖。

【0019】圖6是根據本案內容的態樣圖示HMM E控制平面模型的第三實例的示意圖。

【0020】圖7和8是根據本案內容的態樣圖示使用單個連線性上下文在客戶端設備與網路之間執行的用以建立複數個單獨的服務上下文的第一訊號傳遞程序的撥叫流程圖。

【0021】圖9是根據本案內容的態樣圖示封裝的非存取層（NAS）訊息的示意圖。

【0022】圖10和11是根據本案內容的態樣圖示使用單個連線性上下文在客戶端設備與網路之間執行的用以建立複數個單獨的服務上下文的第二訊號傳遞程序的撥叫流程圖。

【0023】圖12是圖示使用作為代理的HMM E的eNB與SME之間的S1AP（S1應用協定）通訊的實例的示意圖。

【0024】圖13是圖示使用穿過HMM E的安全隧道的eNB與SME之間的S1AP通訊的實例的示意圖。

【0025】圖14是根據本案內容的態樣圖示具有擴展的使用者平面安全性的HMM E控制平面模型的實例的示意圖。

【0026】圖15是根據本案內容的態樣圖示HMM E資料平面模型的第一實例的示意圖。

【0027】圖16是根據本案內容的態樣圖示HMM E資料平面模型的第二實例的示意圖。

【0028】圖17是根據本案內容的態樣圖示HMM E資料平面模型的第三實例的示意圖。

【0029】圖18是根據本案內容的態樣圖示使用者平面安全性終止的實例的示意圖。

【0030】圖19和20是根據本案內容的態樣圖示在客戶端設備處可操作以利用單個連接來建立多個服務上下文的示例性方法的流程圖。

【0031】圖21和22是根據本案內容的態樣圖示在連線性網路的網路節點處可操作以與客戶端建立單個連接用於支援多個服務網路的示例性方法的流程圖。

【0032】圖23是根據本案內容的態樣圖示在服務網路的網路節點處可操作以使用與連線性網路的單個連接來

與客戶端設備建立多個安全性上下文的示例性方法的流程圖。

**【實施方式】**

**【0033】** 下文結合附圖闡述的具體實施方式意欲作為各種配置的描述，並不意欲表示在其中可以實踐本文描述的概念的僅有配置。具體實施方式包括出於提供對各個概念的透徹理解的目的的具體細節。但是，對於本發明所屬領域中具有通常知識者來說顯而易見的是，可以在沒有這些具體細節的情況下實踐這些概念。在一些實例中，為了避免使此類概念模糊，以方塊圖的形式圖示公知的結構和組件。

**【0034】** 本案內容的態樣提供了用於在共用單個連線性上下文時實現多個連線性和服務上下文以建立網路連接的安全模型。網路連接可以包括單個無線電或無線鏈路，其可以支援使用多個不同的服務上下文和安全性上下文的多個服務連接。單個無線電或無線鏈路可以包括與單個連線性上下文相對應的一或多個無線通道、頻率或載波。通常，上下文（例如，連線性上下文、服務上下文、安全性上下文）是描述在兩個或兩個以上實體之間建立的連接、服務或安全性的資訊集合。在本案內容的一個態樣中，連線性上下文包括進化型封包系統（EPS）行動性管理（EMM）上下文、或EMM上下文和EPS通信期管理（ESM）上下文二者。

【0035】 在本案內容的一個態樣中，可以基於單個連線性上下文（例如，E M M上下文）在客戶端設備（例如，U E）與無線存取網路（R A N）之間建立無線電資源控制（R R C）鏈路或媒體存取控制（M A C）鏈路。在一個實例中，R A N可以是蜂巢R A N或包括W i - F i存取點的無線電網路，或者蜂巢和W i - F i無線電單元的組合。在另一個實例中，R A N可以具有在經許可及/或免許可頻譜中操作的並且由公共無線電資源控制（R R C）或媒體存取控制（M A C）機制控制的一或多個無線電存取節點。在各個實例中，R R C可以包括蜂巢R R C、蜂巢R R M（無線電資源管理）、媒體存取控制（M A C）或用於經由一或多個鏈路控制對無線電資源的存取（包括針對較高層訊號傳遞和使用資料的傳輸的無線電資源的建立）的任何其他訊號傳遞機制。

【0036】 在建立了單個連線性上下文（例如，E M M上下文）之後，客戶端設備可以使用受到不同安全性上下文保護的多個不同的服務上下文來在單個鏈路上建立同時的或併發的服務連接。在一個實例中，服務上下文包括E S M上下文。以此方式，共用的單個連線性上下文被用於較低層級的無線鏈路連接，而兩個或兩個以上服務上下文被用來在無線電鏈路上例如與服務提供者建立服務連接。本案內容的態樣提供用於保護服務連接同時共用到R A N的單個鏈路或連接的安全模型。

支援多個服務連接的單個連線性連接

【0037】圖1圖示客戶端設備102（例如，UE）與無線電存取網路（RAN）120之間的單個無線電鏈路101，其可以用來將客戶端設備102耦合到兩個或兩個以上服務提供者104或供應功能單元104和106，同時支援與不同服務上下文108、110和112相關聯的多個服務連接114、116、118。在該特定實例中，在客戶端設備102處實現的單個連線性上下文122可以被用來與RAN 120建立無線電鏈路101。無線電鏈路101可以由與不同的服務上下文108、110和112相關聯的多個同時的連接來共用。單個連線性上下文（例如，EMM上下文或EMM/ESM上下文）被用來與網路主行動性管理實體124（HMM E）建立連接，該網路HMM E提供：安全性、用於承載管理和資料連接管理的訊號傳遞、傳呼、行動性等等。對單個連線性上下文122的使用有助於在同一無線電鏈路101上對具有相應服務連接114、116和118的多個同時的或併發的服務上下文108、110、112的使用。服務連接之每一者服務連接可以利用不同的安全性上下文來保護（例如，在圖4-6和14-18中示出的）。在一個實例中，若客戶端設備102具有三種類型的訂閱（例如，三種服務上下文），則這可以實現用於在客戶端設備102與RAN 120之間的單個（同一個）無線電鏈路101上建立三個同時的服務連接114、116和118的能力：每個訂閱及/或服務上下文108、110和112對應於一個連接。單個無線電鏈路可以包括一或多個無線電承載。同時的服務連接114、

116 及 / 或 118 中的任何一或多個在任何給定的時間可以是閒置的或活動的。

【0038】主 MME 124 (HMM E) 可以在邏輯上靠近 RAN 120 來實現並且用來管理連線性上下文 (例如, EMM 上下文或 EMM/ESM 上下文) 的建立, 以及基於共享的連線性上下文 122 來建立無線電鏈路 101。主 MME 124 可以用來認證客戶端設備 102 以建立連線性上下文。例如, 主 MME 124 可以在控制平面上執行與客戶端設備 102 的非存取層 (NAS) EPS 行動性管理 (EMM) 以控制客戶端設備 102 的行動性及 / 或安全性。主 MME 124 亦可以在控制平面上與客戶端設備 102 執行非存取層 (NAS) EPS 通信期管理 (ESM) 以支援或配置服務連接 114、116、118。主 MME 124 可以與歸屬授權、認證和計費 (H-A A A) 伺服器 144 認證客戶端設備 102 以基於與客戶端設備 102 相關聯的憑證和訂閱資訊來決定連線性上下文 122 是否應當被建立。例如, 客戶端設備 102 可以具有用於儲存憑證和訂閱資訊的 SIM 卡。因此, 連線性上下文 122 用來建立能夠由客戶端設備 102 的多個服務連接 114、116 和 118 共享的單個無線電鏈路 101。

NAS 安全性

【0039】在本案內容的一個態樣中, 修改非存取層 (NAS) 模型以實現單獨的 EMM 上下文和 ESM 上下文。例如, 能夠在沒有 ESM 上下文的情況下利用 HMM E 建立 EMM 上下文。HMM E 是可以位於靠近 RAN 的核心

網路實體。客戶端（例如，UE）可以具有用於建立不同上下文的不同憑證。例如，被用來建立 EMM 上下文的憑證可以不同於被用來建立 ESM 上下文的憑證。憑證可以用於決定客戶端是否能夠建立所請求的 EMM 上下文及 / 或 ESM 上下文的資訊，其可以被儲存在客戶端及 / 或網路節點處。例如，連線性憑證被用來建立 EMM 上下文，而服務憑證被用來建立 ESM 上下文。不同的服務憑證可以被用來建立不同的 ESM 上下文。在一個實例中，NAS 模型使用相同的憑證集合在 HMM E 處同時地實現對 EMM 上下文和一或多個 ESM 上下文（例如，圖 1 的連線性上下文 122 和 EMM / ESM 上下文 126）的建立。

【0040】 參考圖 1，一旦建立了連線性上下文 122（亦即，在單個無線電鏈路 101 上建立到網路的连接），客戶端設備 102 就可以基於相應的憑證集合（例如，不同的服務憑證）與不同的網路實體建立一或多個 ESM 上下文，憑證集合允許經由連線性提供者中的可區分的連接管理實體的服務區分。連接管理實體的實例是服務管理實體（SME）。

【0041】 在本案內容的一個態樣中，RAN 120 可以被連接到複數個服務提供者 104 和 106。例如，每個服務提供者 104、106 可以包括具有服務管理實體（SME）128 和 130 的連線性提供者以及一或多個封包資料網路閘道（P-GW）和一或多個服務閘道（S-GW）132 和 134。這些 SME 128 和 130 之每一者可以維護用於服務連接

1 1 4 和 1 1 6 的 各 自 的 E S M 上 下 文 1 3 6 和 1 3 8，其中服務連接 1 1 4 和 1 1 6 是 使 用 可 以 由 相 應 的 服 務 A A A（授 權、認 證 和 計 費）伺 服 器 提 供 的 憑 證 和 訂 閱 資 訊 建 立 的。例 如，S M E 1 2 8 和 1 3 0 可 以 經 由 各 自 的 服 務 A A A 伺 服 器 1 4 0 和 1 4 2 或 經 由 其 支 援 認 證 客 戶 端 設 備 1 0 2，以 基 於 與 服 務 上 下 文 1 0 8 和 1 1 0 相 關 聯 的 並 且 由 A A A 伺 服 器 1 4 0 和 1 4 2 提 供 的 憑 證 來 決 定 服 務 連 接 1 1 4 及 / 或 1 1 6 是 否 應 當 被 建 立。成 功 的 認 證 使 得 S M E 能 夠 為 客 戶 端 設 備 1 0 2 建 立 服 務 上 下 文 1 0 8 和 1 1 0（例 如，E S M 上 下 文）。相 應 的 服 務 上 下 文（E S M 上 下 文 1 3 6、1 3 8）可 以 在 S M E 1 2 8 和 1 3 0 處 建 立。

【0 0 4 2】在圖 1 的示例性說明中，客戶端設備 1 0 2 已經建立了第一服務上下文 1 0 8、第二服務上下文 1 1 0 和第三服務上下文 1 1 2。但是，可以預期的是客戶端設備 1 0 2 可以建立任何數量的服務上下文。

【0 0 4 3】在圖 1 中，客戶端設備 1 0 2 和多個服務提供者（例如，服務網路 1 0 4 及 / 或 1 0 6）可以建立多個服務上下文 1 0 8、1 1 0 和 1 1 2，其中每個服務上下文 1 0 8、1 1 0 和 1 1 2 可以與一或多個憑證集合相對應。憑證集合可以被定義為或者包括使得其他設備（例如，網路設備）能夠向服務或連接辨識客戶端設備 1 0 2（或者客戶端設備的使用者 / 用戶）的資訊集合、被用於認證的安全金鑰等等。憑證可以被實現為安全性上下文。例如，被儲存在客戶端設

備處的認證資訊和被儲存在網路側的相應的資訊可以被稱為安全性上下文。

【0044】 在一個實例中，基於多個同時的服務上下文108、110和112的连接114、116和118可以被覆用在與RAN 120的單個連接上，例如，通訊協定堆疊的層2連接（例如，LTE層2）。服務上下文108、110和112是基於由客戶端設備102用於建立每個服務上下文108、110和112的具體的/不同的標識來區分的。例如，客戶端設備102可以被供應有憑證集合，憑證集合提供對與主MME的連線性建立（亦即，至少EMM上下文）的安全存取，該主MME提供到網路的訊號傳遞或連接並且實現行動性管理。此類憑證可以是，例如，開箱即用憑證、服務供應商憑證或由OEM（原始設備製造商）提供的並且在製造時由製造客戶端設備102的實體安裝在客戶端設備102中的憑證。對OEM憑證的使用使得OEM能夠提供憑證並且託管針對此類憑證的認證，從而使得客戶端設備102能夠支援不同的服務提供者，因為服務提供者憑證被用來僅提供ESM上下文而不是EMM上下文或連線性上下文。隨著OEM憑證用於第一（EMM）上下文（例如，連線性上下文）的建立，有可能建立提供訊號傳遞，行動性管理、安全性等等的EMM（連線性）上下文而不給建立此類連線性帶來收費或費用，因為沒有產生關於該上下文的資料傳輸量或訊息。

【0045】 服務相關的憑證被用來與SME（服務管理實體）建立一或多個ESM上下文（例如，服務上下文）。在各種配置中，SME可以實體地與HMM E分開，該SME（或SME功能的軟體版本）可以共置在或者託管在HMM E處或者其組合，其中一些SME可以被HMM E共置/託管，而其他SME與HMM E分開。在一些實例中，UE可以利用連線性憑證來建立ESM上下文。

#### AS 安全性

【0046】 存取層（AS）是經由RAN 120處理客戶端設備102（例如，UE）與核心網路（CN）之間的活動的功能層和協定集合。例如，CN可以包括HMM E 124、一或多個SME 128、130、一或多個S-GW 132、134和一或多個P-GW 132、134。在AS中，可以在CN與客戶端設備102之間建立多個無線電存取承載（RAB）。在本案內容的一個態樣中，每個RAB可以與不同的ESM上下文相關聯，並且每個ESM上下文可以由虛擬ESM（VESM）標籤（或辨識符）來決定。在本案內容的一個態樣中，多個RAB與同一EMM上下文相關聯。在該情況下，RAN 120（例如，進化型節點B或eNB）無法看見多個ESM上下文。亦即，RAN 120可能不能在EMS上下文中區分資料傳輸量。eNB具有RAB集合，例如，一些對應於第一ESM上下文，以及一些對應於第二ESM上下文，並且HMM E具有RAB到具體ESM上下文的映射。

【0047】在圖1中，RAN 120被描述為存在於存取層內。但是，RAN 120亦提供NAS功能。在由存取層提供的服務之中是NAS實體（例如，客戶端設備和核心網路節點）之間的NAS訊息的傳輸。NAS協定支援客戶端設備的行動性以及用於建立和維護客戶端設備與核心網路之間的連接的程序。例如，NAS協定可以被用來傳輸客戶端設備102與圖1中圖示的服務提供者A的核心網路（CN）及/或服務提供者B的CN之間的NAS訊息。儘管存取層（AS）傳輸NAS訊號傳遞，但是NAS訊號傳遞並不終止於存取層處。在本案內容的一個態樣中，客戶端設備102與RAN 120之間的單個無線電鏈路101（例如，RRC鏈路）可以被邏輯地或者虛擬地分成多個服務連接，例如，服務連接114和116。服務連接是與它們相應的服務上下文（例如，ESM上下文136和138）相關聯地建立的。

#### 設備辨識符

【0048】各個客戶端設備辨識符可以被用來在AS及/或NAS中辨識客戶端設備102（例如，UE），以便經由單個鏈路實現多個服務連接。一些非限制性實例包括國際行動用戶標識（IMSI）、全球唯一臨時UE標識（GUTI）、用戶服務標識（SCSI）、臨時SCSI（T-SCSI）、全球唯一臨時通信期標識（GUTSI）和臨時傳輸辨識符（TTI）。例如，在連線性上下文122中，客戶端設備102的GUTI可以被映射到在客戶端設備中活動的每個服務

上下文（例如，服務上下文 108、110 和 112）的 GUTSI。因此，基於服務上下文到不同服務提供者的連接可以由 HMM E 124 使用適當的客戶端設備辨識符來辨識。

【0049】 在本案內容的一個態樣中，SCSI 可以是客戶端設備（UE）提供給 SME 用於認證的永久性標識（類似於典型的 UE-MME 認證中的 IMSI）。SCSI 可以辨識具體的 UE 訂閱和相關憑證。SCSI 可以被 SME 用來辨識 AAA 或認證/授權伺服器，該 AAA 或認證/授權伺服器被用來取回相應的客戶端訂閱簡檔並且認證客戶端設備。

【0050】 在本案內容的一個態樣中，T-SCSI 可以是臨時辨識符，該臨時辨識符可以被分配以在客戶端設備與 SME 之間的後續訊號傳遞中辨識該客戶端設備（例如，UE）。在一些實例中，T-SCSI 可能不總是被使用及/或可能不總是被分配。若 SME 向客戶端設備提供 T-SCSI，則客戶端設備可以將其用在客戶端設備與 SME 之間的後續訊號傳遞中。

【0051】 在本案內容的一個態樣中，在成功的認證時，GUTSI 可以由 SME 分配給客戶端設備。GUTSI 可以由客戶端設備用在客戶端設備與相同 SME 之間交換的所有訊號傳遞或資料中。在一個實例中，客戶端設備在 NAS 載荷（其包含該客戶端設備與 SME 之間的實際訊息）之外提供所分配的 GUTSI，以辨識在客戶端設備與 HMM E 之間傳輸的 NAS 載荷屬於哪個客戶端設備。在另一個實例中，客戶端設備可以在 NAS 載荷之內提供 GUTSI。

H M M E 可以使用 G U T S I 區分及 / 或辨識從客戶端設備發送的訊號傳遞被指向哪個 S M E 。例如，當 U E - S M E N A S 訊息被封裝在客戶端設備（例如，U E ）與 H M M E 之間的 N A S 訊息中時，該客戶端設備提供與該 U E - S M E N A S 訊息相關聯的 G U T S I ，以向 H M M E 指示要向哪個 S M E 發送 N A S 訊息以及 U E - S M E N A S 訊息與哪個客戶端設備相對應。

【 0 0 5 2 】 在本案內容的一個態樣中，臨時傳輸辨識符（ T T I ）可以被 S M E 分配用於客戶端設備與 S M E 之間的服务上下文，以便在 H M M E 中辨識客戶端設備的 E S M 上下文與相應的 S M E 之間的關係。在接收到包含 T T I 的訊號傳遞時，H M M E 使用 T T I 來辨識相應的客戶端設備或 S M E ，並且將訊號傳遞轉發給所辨識的客戶端設備或 S M E 。

【 0 0 5 3 】 在本案內容的一個態樣中，客戶端設備可以在針對建立服務連接或服务上下文的請求期間，提供由客戶端設備用來辨識正在針對其請求服務上下文建立的網路或服务 的辨識符。這可以是存取點名稱（ A P N ）或服务的任何適當的辨識符。上述設備辨識符在本質上是說明性的而非限制性的。在本案內容的其他態樣中，其他適當的設備辨識符可以被用來有助於客戶端設備與 H M M E / S M E 之間的通訊。

示例性客戶端設備

【0054】圖2圖示被配置為使用單個無線電鏈路來支援多個同時的服務上下文或連接的示例性客戶端設備202。客戶端設備202可以是與圖1、4-8、10、11和14-18中描述的UE或客戶端設備中的任何UE或客戶端設備相同的UE或客戶端設備。客戶端設備202可以包括被操作地耦合至彼此的無線網路通訊介面204、一或多個處理器206和記憶體/儲存208。客戶端設備202的各種功能可以被實現在軟體、韌體、硬體或其任何組合中。

【0055】無線網路通訊介面204可以用來使用有助於建立到其他設備/網路/服務的無線鏈路或連接的一或多個無線電存取技術，經由一或多個無線電存取網路將客戶端設備202連接到一或多個實體或網路。在一個實例中，無線網路通訊介面204可以被配置為有助於客戶端設備202與其他無線實體或網路的無線通訊。無線網路通訊介面204可以包括一或多個接收器模組/電路/功能單元226、一或多個發射器模組/電路/功能單元228及/或一或多個天線模組/電路/功能單元230。接收器226、發射器228和天線230可以被操作地耦合至彼此。一或多個天線230可以有助於與一或多個無線設備、網路及/或服務的無線通訊。

【0056】處理器206可以被操作地耦合到無線網路通訊介面204。處理器206可以包括無線電鏈路建立模組/電路/功能單元210、服務上下文建立模組/電路/功能單

元 2 1 2 和使用者平面（U P）安全性上下文建立模組 / 電路 / 功能單元 2 1 3。

【0 0 5 7】處理器 2 0 6 可以被配置用於處理，包括對可以被儲存在記憶體 / 存放裝置 2 0 8 上的電腦可執行代碼或程式編制的執行。記憶體 / 存放裝置 2 0 8 可以包括無線電鏈路建立指令 2 1 6、服務上下文建立指令 2 1 8 和安全性上下文建立指令 2 1 9。在一些實例中，記憶體 / 存放裝置 2 0 8 亦可以儲存連線性上下文 2 3 2、一或多個服務上下文 2 3 4、一或多個安全性上下文 2 3 5 和被處理器 2 0 6 使用的其他資料。

【0 0 5 8】客戶端設備 2 0 2 可以被用來實現圖 7 - 1 1 和 1 9 - 2 0 中示出的功能及 / 或程序中的一或多個。

示例性網路節點

【0 0 5 9】圖 3 圖示被配置為實現用於支援客戶端設備在單個無線電鏈路上操作的 H M M E 及 / 或 S M E 的示例性網路節點 3 0 2，該單個無線電鏈路支援多個服務上下文的同時的或併發的操作。網路節點 3 0 2 可以是與圖 1、4 - 8 和 1 0 - 1 8 中描述的網路節點或實體中的任何網路節點或實體相同的網路節點或實體。網路節點 3 0 2 可以包括可以被操作地耦合至彼此的網路通訊介面 3 0 4、一或多個處理器 3 0 6 和記憶體 / 儲存 3 0 8。

【0 0 6 0】網路通訊介面 3 0 4 可以用來使用有助於在客戶端設備與網路節點之間建立鏈路的一或多個有線或無

線存取技術，將網路節點302耦合到一或多個網路或客戶端設備。網路通訊介面304可以包括至少一個接收器模組/電路/功能單元326及/或至少一個發射器模組/電路/功能單元328。網路通訊介面304亦可以包括被操作地耦合到至少一個接收器326及/或至少一個發射器328的一或多個天線模組/電路/功能單元330。

【0061】 處理器306可以被操作地耦合到網路通訊介面304。處理器306可以包括無線電鏈路建立模組/電路/功能單元310和HMM E模組/電路/功能單元312。

【0062】 處理電路306可以被配置用於處理，包括對可以被儲存在記憶體/儲存308上的指令的執行。如本文使用的，無論被稱為軟體、韌體、中介軟體、微代碼、硬體描述語言或者其他術語，術語「指令」可以被廣泛地解釋為包括但不限於指令集合、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。

【0063】 記憶體/儲存308可以被操作地耦合到處理器306，並且亦可以被操作地耦合到網路通訊介面304。記憶體/儲存308可以包括無線電鏈路建立指令316和HMM E/SME指令318。

【0064】 在一些實例中，記憶體/儲存308可以儲存連線性上下文（或憑證）332、服務上下文（或憑證）334及/或安全性上下文335。另外，在一些實現方式中，處

理器 306 可以在具有或不具有 HMM 模組 312 的情況下實現服務管理實體 (SME) 模組/電路/功能單元 314。

【0065】 網路節點 302 可以實現圖 7、8、10-13 和 22-22 中示出的功能及/或程序中的一或多個。在一個特定的實例中，網路節點 302 可以實現關於圖 20 描述的程序中的一或多個。

### HMM 控制平面模型

【0066】 在各個實例中，客戶端設備可以基於 HMM 處的單個 EMM 上下文與存取網路（例如，RAN）建立連接或連线性。一旦連线性被建立，客戶端設備就與不同 SME 建立對應於不同的憑證集合的一或多個 ESM 上下文。圖 4-6 是根據本案內容的一些態樣圖示用於有助於 EMM 上下文和 ESM 上下文的建立的 HMM 控制平面模型的一些實例的圖。

【0067】 在圖 4 中示出的第一 HMM 控制平面模型中，客戶端設備 402（例如，UE）經由使用例如連线性憑證和歸屬授權、認證和計費（AAA）伺服器 407 相互認證，與 HMM/SME 406 建立 EMM 上下文 404（連线性上下文）。單個 EMM 上下文 404 有助於客戶端設備 402 與 RAN 403（例如，eNB）之間的單個無線電鏈路的建立。一旦 EMM 上下文 404 已經被建立，客戶端設備 402 就可以使用多個服務憑證和 AAA 伺服器 407、413、415 與多個 SME（HMM/SME 406、SME 412、SME 414）

建立一或多個ESM上下文408（ESM上下文1、2、3）。客戶端設備402與HMME 406之間的NAS訊息（針對HMME功能）可以基於被儲存在HMME 406中的預設的連線性安全性上下文（例如，NAS安全性上下文）來進行加密和完整性保護。客戶端設備402與SME之間的NAS訊息是使用分別被儲存在SME中的不同的安全性上下文410（NAS安全性上下文）來加密和完整性保護的。客戶端設備402和每個SME使用相應的服務憑證來相互認證。在圖4的該實例中，第一ESM上下文（ESM上下文1）是使用第一安全性上下文（安全性上下文1）來保護的，第一安全性上下文被儲存在客戶端設備402和第一SME 406中。第二ESM上下文（ESM上下文2）是使用第二安全性上下文（安全性上下文2）來保護的，該第二安全性上下文被儲存在客戶端設備402和第二SME 412中。第三ESM上下文（ESM上下文3）是使用第三安全性上下文（安全性上下文3）來保護的，該第三安全性上下文被儲存在客戶端設備402和第三SME 414中。

【0068】 HMME/SME 406被配置為選擇第一服務/封包資料閘道（S/P GW）418，該第一S/P GW 418被連接到第一服務網路420。類似地，第二SME 412被配置為選擇第二S/P GW 422，該第二S/P GW 422被連接到第二服務網路424。同樣地，第三SME 414被配置為選擇第三S/P GW 426，該第三S/P GW 426被連接到第三服務網路428。第一服務網路420、第二服務網

路 4 2 4 和 第三服務網路 4 2 8 可以由相同的服務提供者或不同的服務提供者運營。在一些實例中，服務閘道（S - G W）的選擇可以由 H M M E 4 0 6 來執行。在此類情況下，H M M E 4 0 6，例如在服務請求期間向該 S M E 通知所選擇的 S - G W。

【0 0 6 9】服務網路可以是至少部分地在連線性網路（例如，包括單個無線電鏈路 4 3 0 和 R A N 4 0 3）中建立的虛擬網路，並且一或多個服務網路與由一或多個服務提供者（例如，服務網路 1、2 和 3）提供的具體的或不同的服務相關聯。在一個特定的實例中，第一虛擬網路包括無線電鏈路 4 3 0、R A N 4 0 3、第一 H M M E / S M E 4 0 6、第一 S / P G W 4 1 8 和第一服務網路 4 2 0。在另一個實例中，第二虛擬網路包括無線電鏈路 4 3 0、R A N 4 0 3、H M M E 4 0 6、第二 S M E 4 1 2、第二 S / P G W 4 2 2 和第二服務網路 4 2 4。在另一個實例中，第三虛擬網路包括無線電鏈路 4 3 0、R A N 4 0 3、H M M E 4 0 6、第三 S M E 4 1 4、第三 S / P G W 4 2 6 和第三服務網路 4 2 8。

【0 0 7 0】圖 5 根據本案內容的態樣圖示第二 H M M E 控制平面模型。第一 H M M E 控制平面模型和第二 H M M E 控制平面模型是相似的，並且因此為了簡潔可以省略冗餘的描述。客戶端設備 4 0 2 與 H M M E 4 0 6 建立 E M M 上下文 4 0 4。一旦 E M M 上下文 4 0 4 已經被建立，客戶端設備 4 0 2 就可以使用多個服務憑證和 A A A 伺服器 4 0 7、4 1 3、4 1 5 與多個 S M E（H M M E / S M E 4 0 6、S M E 4 1 2、S M E 4 1 4）

建立一或多個ESM上下文408（ESM上下文1、2、3）。客戶端設備402和每個SME 406、412、414可以使用相應的服務憑證來相互認證。例如，客戶端設備402可以使用針對SME的三個不同的憑證。在圖5的第二HMME控制平面模型中，HMME 406可以直接選擇並且控制服務連接的服務/封包資料閘道（例如，S/P GW 1、2、3）。這不同於圖4的第一HMME控制平面模型，在該模型中SME選擇服務/封包資料閘道。在本案內容的另一個態樣中，SME（例如，SME 412和SME 414）可以選擇S/P GW並且將選擇轉發給HMME 406，該HMME 406選擇所選擇的S/P GW。

【0071】圖6根據本案內容的態樣圖示第三HMME控制平面模型。第一HMME控制平面模型和第三HMME控制平面模型是相似的，並且因此為了簡潔可以省略冗餘的描述。客戶端設備402與HMM 406建立EMM上下文404。一旦EMM上下文404已經被建立，客戶端設備402就可以使用多個服務憑證和AAA伺服器407、413、415與多個SME（HMME/SME 406、SME 412、SME 414）建立一或多個ESM上下文408（ESM上下文1、2、3）。客戶端設備402和每個SME可以使用服務憑證來相互認證。例如，客戶端設備402可以具有針對服務連接的不同的服務憑證。在第三HMME控制平面模型中，HMME 406可以基於ESM上下文408（例如，ESM上下文1、2、3）選擇服務閘道（S-GW）431。隨後，S-GW 431基

於 E S M 上下文 4 0 8 選擇封包資料閘道（ P - G W 4 3 2 、 4 3 4 、 4 3 6 ）。這不同於圖 4 的第一 H M M E 控制平面模型，在該模型中 S M E 選擇服務和封包資料閘道。在一些實例中，S M E（例如，S M E 4 1 2 和 S M E 4 1 4）可以選擇封包資料閘道（例如，P - G W 1、2、3）並且可以經由 H M M E 4 0 6 將選擇轉發給 S - G W 4 3 1。隨後，S - G W 4 3 1 選擇相應的封包資料閘道。在圖 4 - 6 的 H M M E 控制平面模型中，不同的服務連接可以利用不同的安全性上下文 4 1 0（例如，安全性上下文 1、2、3）來保護。

【0 0 7 2】圖 7 - 8 是根據本案內容的態樣圖示用於使用單個連線性上下文建立多個服務上下文的程序的撥叫流程圖 5 0 0。在一個實例中，程序可以由 U E（客戶端設備）5 0 2、e N B 5 0 4、H M M E 5 0 6、S M E 5 0 8、服務閘道（S - G W）5 1 0、第一封包資料閘道（P - G W）5 1 2、第二 P - G W 5 1 4、第一歸屬用戶伺服器（H S S）5 1 6 和第二 H S S 5 1 8 來執行。如撥叫流程圖 5 0 0 中示出的，使用單個連線性上下文（例如，E M M 上下文）在 U E 5 0 2 與網路（例如，e N B 5 0 4）之間建立無線電鏈路或連接，隨後其被複數個服務上下文（例如，S M E 上下文）共享。U E 5 0 2、e N B 5 0 4、H M M E 5 0 6、S M E 5 0 8、S - G W 5 1 0、第一 P - G W 5 1 2、第二 P - G W 5 1 4、第一 H S S 5 1 6 和第二 H S S 5 1 8 可以是與圖 1 - 6 和 1 4 - 1 8 中的任何一個中示出的那些相同的設備。

【0073】 UE 502 嘗試經由向 eNB 504 發送附著請求 520 來附著到網路，eNB 504 在初始 UE 訊息 522 中將該請求發送或轉發給 HMM E 506。初始 UE 訊息可以包括 UE ID，使得 HMM E 506 可以辨識客戶端設備 502。UE ID 可以是上文描述的設備辨識符中的任何設備辨識符。HMM E 506 決定 UE 502 是否具有針對所請求的連接的恰當的憑證。例如，HMM E 506 可以經由與第一 HSS 516 執行進化型封包系統 (EPS) 認證和金鑰協商 (AKA) 程序 524 來檢查 UE 502 是否被允許附著。例如，第一 HSS 516 可以經由產生認證向量並且將其發送給 HMM E 506，隨後 HMM E 506 代表第一 HSS 516 執行與 UE 502 的認證來獲得 MME 基本金鑰。隨後，HMM E 506 經由交換 NAS 安全性模式命令 (SMC) 訊息 526 與 UE 502 執行 NAS 安全性建立程序。若 NAS SMC 被完成，則 UE 502 與 HMM E 506 之間的 NAS SMC 訊息可以例如基於被儲存在 HMM E 506 中的 NAS 安全性上下文 (若被建立) 來進行加密和完整性保護。接下來，HMM E 506 基於 S-GW 選擇功能來選擇 S-GW 510 並且為 UE 502 的預設承載分配 EPS 承載標識。隨後，HMM E 506 向所選擇的 S-GW 510 發送建立通信期請求 528。作為回應，S-GW 510 在其 EPS 承載表中建立新的條目並且向第一 P-GW 512 發送建立通信期請求訊息 529。

【0074】 回應於建立通信期請求訊息 529，第一 P-GW 512 可以在其 EPS 承載表中建立新的條目並且產生收費

ID。隨後，第一P-GW 512向S-GW 510和HMM E 506發送建立通信期回應訊息530。接下來，HMM E 506向eNB 504提供包含附著接受訊息的初始上下文建立請求訊息532。接下來，eNB 504向UE 502發送RRC連接重新配置訊息534，其包括EPS無線電承載標識和附著接受訊息。作為回應，UE 502向eNB 504發送RRC連接重新配置完成訊息536。作為回應，eNB 504向HMM E 506發送初始建立上下文回應訊息538。

【0075】 使用上述程序，UE 502能夠與HMM E 506建立EMM上下文或連線性。例如，程序可以與圖4中示出的第一HMM E控制平面模型一起使用。在EMM上下文被建立之後，UE 502可以使用下列關於圖8描述的程序建立一或多個SME上下文。

【0076】 參考圖8，為了建立服務的ESM上下文或服務連接，UE 502向HMM E 506發送包括服務辨識符（服務ID）的服務註冊訊息540。在接收到服務註冊訊息540時，HMM E 506基於由UE 502提供的服務ID來選擇SME（例如，SME 508）並且向所選擇的SME 508發送初始UE訊息542。初始UE訊息542可以包括如前述的客戶端設備辨識符（例如，SCSI），使得SME 508可以辨識UE 502。SME 508可以經由與第二HSS 518執行EPS-AKA程序544來檢查UE 502是否具有服務的訂閱。例如，第二HSS 518可以經由產生認證向量並且將其發送給SME 508，隨後SME 508代表第二HSS 518

與 UE 502 執行認證，來獲得金鑰。隨後 SME 508 經由交換 NAS 安全性模式命令（SMC）訊息 546 與 UE 502 執行 NAS 安全性建立程序。

【0077】 UE 502 與 SME 508 之間的 NAS 訊息可以使用 ESM 安全性上下文來保護。例如，UE 502 可以使用與 SME 508 建立的 ESM 安全性上下文來加密並且保護 NAS 訊息。針對 SME 508 的 NAS 訊息被封裝在針對 HMM E 506 的外部 NAS 訊息中（亦即，封裝的 NAS 中的 NAS 訊息）。例如，外部 NAS 訊息是使用 UE 502 與 HMM E 506 之間建立的安全性上下文來進行加密和完整性保護的。在一個實例中，參考圖 9，針對 HMM E 的封裝的 NAS 中的 NAS 訊息 600 可以包括 SME ID 602，用於使得 HMM E 能夠辨識內部 NAS 訊息 604 被轉發到的 SME 508，以及 UE ID 606（其可以由 SME 來指派）用於使得 SME 508 能夠辨識 UE 502。在一個實例中，UE ID 606 可以包括已經被 SME 分配的 GUTI 或 GUTSI（或其他適當的辨識符）。

【0078】 類似地，SME 508 可以使用 ESM 安全性上下文來對 NAS 訊息進行加密和保護。隨後，該 NAS 訊息（例如，內部 NAS 訊息 604）被封裝在 HMM E 506 的外部 NAS 訊息（或可以被定義的任何其他適當的容器）中。在一個實例中，外部 NAS 訊息可以是不受保護的，但是經由安全的通道被傳輸給 HMM E 506。在一個實例中，HMM E 506 和 SME 508 可以為安全的通訊建立 IP 安全

性（IPsec）通道。外部NAS訊息可以包括UE ID，用於使得HMM E 506能夠將UE ID映射到S1-AP UE ID。在另一個實例中，外部NAS訊息可以使用HMM E 506的E MM安全性上下文來進行加密和完整性保護。

【0079】隨後，SME 508向S-GW 510發送建立通信期請求548。作為回應，S-GW 510在其EPS承載表中建立新的條目，並且向第二P-GW 514發送建立通信期請求訊息。回應於建立通信期請求訊息，第二P-GW 514可以在其EPS承載表中建立新的條目並且產生收費ID。隨後，第二P-GW 514向S-GW 510和SME 508發送建立通信期回應訊息550。接下來，SME 508向HMM E 506提供包含附著接受訊息的初始上下文建立請求訊息552。HMM E 506將初始上下文建立請求訊息554轉發給eNB 504。接下來，eNB 504向UE 502發送包括EPS無線承載標識和附著接受訊息的RRC連接重新配置訊息556。作為回應，UE 502向eNB 504發送RRC連接重新配置完成訊息558。接下來，eNB 504向HMM E 506發送初始建立上下文回應訊息560，HMM E 506將初始建立上下文回應訊息562轉發給SME 508。利用上文描述的程序，與SME 508建立SME上下文。

【0080】此外，AS安全性模式命令（SMC）訊息可以被用來在UE 502與eNB 504之間建立AS安全性上下文。基於AS安全性上下文（例如，圖15-17中示出的AS安全性上下文），UE 502和eNB 504能夠保護空中傳

輸量。儘管單個無線電鏈路（例如，圖1的單個鏈路101）被用於多個服務連接，但是每個服務連接可以利於基於相應的AS安全性上下文的單獨的金鑰來保護，並且由相應的虛擬ESM（VESM）標籤來區分。

【0081】圖10-11是根據本案內容的態樣圖示用於使用單個連線性上下文來建立多個服務上下文的程序的撥叫流程圖700。在一個實例中，程序可以由UE（客戶端設備）702、eNB 704、HMME 706、SME 708、服務閘道（S-GW）710、第一封包資料閘道（P-GW）712、第二封包資料閘道P-GW 714、第一歸屬使用者伺服器（HSS）716和第二HSS 718來執行，以使用UE 702處的單個連線性上下文（例如，EMM上下文）來建立無線電鏈路或連接，隨後其被複數個服務上下文（例如，SME上下文）或服務連接共享。客戶端設備（UE）702、eNB 704、HMME 706、SME 708、S-GW 710、第一P-GW 712、第二P-GW 714、第一HSS 716和第二HSS 718可以是與圖1、4-6和14-18中的任何一個中示出的那些相同的設備。

【0082】流程圖700基本上類似於圖7-8的流程圖500。因此，為了簡潔可以省略冗餘的描述。例如，圖10中示出的訊號傳遞程序在UE 702與HMME 706之間建立EMM上下文，並且基本上是與圖7中示出的那些相同的程序。

【0083】 參考圖11，為了建立服務的ESM上下文或服務連接，UE 702向HMM E 706發送包括服務辨識符（服務ID）的服務註冊訊息720。在接收到服務註冊訊息720時，HMM E 706基於由UE 702提供的服務ID選擇SME（例如，SME 708）並且向所選擇的SME 708發送初始UE訊息722。初始UE訊息722可以包括如前述的客戶端設備辨識符（例如，SCSI），使得SME 708可以辨識UE 702。SME 708可以經由與第二HSS 718執行EPS-AKA程序724來檢查UE 702是否具有服務的訂閱。例如，第二HSS 718可以經由產生認證向量並且將其發送給SME 708，隨後SME 708代表第二HSS 718與UE 702執行認證，來獲得金鑰。隨後SME 708經由交換NAS安全性模式命令（SMC）訊息726與UE 702執行NAS安全性建立程序。

【0084】 UE 702與SME 708之間的NAS訊息可以使用ESM安全性上下文來保護。例如，UE 702可以使用與SME 708建立的ESM安全性上下文來對NAS訊息進行加密和保護。例如，針對SME 708的NAS訊息被封裝在針對HMM E 706的外部NAS訊息中（亦即，封裝的NAS中的NAS訊息）。外部NAS訊息是使用UE 702與HMM E 706之間建立的安全性上下文來進行加密和完整性保護的。針對HMM E 706的封裝的NAS中的NAS訊息可以包括SME ID，用於使得HMM E 706能夠辨識內部NAS訊息被轉發到的SME 708，以及UE ID（其可

以由該 S M E 來指派) 用於使得 S M E 7 0 8 能夠辨識 U E 7 0 2。在一個實例中，U E I D 可以包括已經由 S M E 分配的 G U T I 或 G U T S I (或其他適當的辨識符)。

【0085】 類似地，S M E 7 0 8 可以使用 E S M 安全性上下文來對 N A S 訊息進行加密和保護。隨後，N A S 訊息(內部 N A S 訊息)被封裝在針對 H M M E 7 0 6 的外部 N A S 訊息(或可以被定義的任何其他適當的容器)中。在一個實例中，外部 N A S 訊息可以是不受保護的，但是經由安全的通道被傳輸給 H M M E 7 0 6。在一個實例中，H M M E 7 0 6 和 S M E 7 0 8 可以為安全的通訊建立 I P 安全性 ( I P s e c ) 通道。外部 N A S 訊息可以包括 U E I D，用於使得 H M M E 7 0 6 能夠將 U E I D 映射到 S 1 - A P U E I D。在另一個實例中，外部 N A S 訊息可以使用 H M M E 7 0 6 的 E M M 安全性上下文來進行加密和完整性保護。

【0086】 U E 7 0 2 可以使用下列描述的程序來建立一或多個 S M E 上下文。例如，參考圖 1 1，S M E 7 0 8 經由 H M M E 7 0 6 向 S - G W 7 1 0 發送建立通信期請求 7 2 8。作為回應，S - G W 7 1 0 在其 E P S 承載表中建立新的條目，並且向第二 P - G W 7 1 4 發送建立通信期請求訊息 7 2 8。回應於建立通信期請求訊息，第二 P - G W 7 1 4 可以在其 E P S 承載表中建立新的條目並且產生收費 I D。隨後，第二 P - G W 7 1 4 向 S - G W 7 1 0 發送建立通信期回應訊息 7 3 0，該 S - G W 7 1 0 經由 H M M E 7 0 6 將訊息轉發給 S M E 7 0 8。接下來，H M M E 7 0 6 向 e N B 7 0 4 發送初始上下文

建立請求訊息 732。接下來，eNB 704 向 UE 702 發送包括 EPS 無線承載標識和附著接受訊息的 RRC 連接重新配置訊息 734。作為回應，UE 702 向 eNB 704 發送 RRC 連接重新配置完成訊息 736。接下來，eNB 704 向 HMM E 706 發送初始上下文建立回應訊息 738，該 HMM E 706 將該初始上下文建立回應訊息轉發給 SME 708。

【0087】 使用上述程序，UE 702 能夠與 SME（例如，SME 708）建立一或多個 ESM 上下文或服務連接。例如，程序可以被用在圖 5 和 6 中示出的第二 HMM E 控制平面模型和第三 HMM E 控制平面模型中。

【0088】 在本案內容的態樣中，eNB 與 HMM E / SME 之間的通訊可以使用如 3GPP 規範中定義的 S1AP（S1 應用協定）。S1AP 的實例在 3GPP TS 36.413 — 進化型通用陸地無線電存取網路（E-UTRAN）；S1 應用協定（S1AP）第 12 版中定義。S1AP 訊息可以使用 NDS/IP（網路域安全性/網際網路協定）來保護。NDS/IP 使用 IP 安全性（IPSec）來實現安全域服務。例如，IPSec 隧道可以被用來保護該 eNB 與 HMM E / SME 之間的訊息。

【0089】 在本案內容的態樣中，eNB 與 HMM E 之間的訊息可以使用如在 LTE 標準（例如，3GPP TS 36.413）中定義的 S1AP。參考圖 12，eNB 802 與 SME 804 之間的訊息可以使用 S1AP 來傳送，並且 HMM E 806 可以被實現為 eNB 與 SME 之間的代理。eNB 802、SME 804

和 H M M E 8 0 6 可以是與圖 4 - 8 、 1 0 、 1 1 和 1 4 - 1 8 中描述的那些相同的設備。在該實例中，H M M E 8 0 6 和 S M E 8 0 4 可以使用單獨的 U E I D 。 H M M E 8 0 6 將 H M M E U E I D 轉化為 S M E U E I D ，或者反之亦然。在 e N B 8 0 2 與 H M M E 8 0 6 之間建立 I P S e c 隧道，並且在 H M M E 8 0 6 與 S M E 8 0 4 之間建立另一個 I P S e c 隧道。I P S e c 隧道可以受到 N D S / I P 的保護。但是，本案內容不被限制到用於 e N B 與 H M M E / S M E 之間的通訊的 S 1 A P 。在本案內容的一些態樣中，單獨的通訊協定可以被用在 e N B 與 S M E 之間、H M M E 與 S M E 之間、e N B 與 H M M E 之間或其組合。

【 0 0 9 0 】 參考圖 1 3 ， e N B 9 0 2 與 S M E 9 0 4 之間的 S 1 A P 可以經由隧道穿越 H M M E 9 0 6 來實現。e N B 9 0 2 、 S M E 9 0 4 和 H M M E 9 0 6 可以是與圖 4 - 8 、 1 0 、 1 1 和 1 4 - 1 8 中描述的那些相同的設備。在該實例中，在註冊或服務請求期間，H M M E 9 0 6 向 S M E 9 0 4 提供 e N B I D 和位址。隨後，e N B 9 0 2 和 S M E 9 0 4 可以基於預先安裝的憑證（例如，證書）來建立安全通道 9 0 8 。在一個特定的實例中，安全通道 9 0 8 可以是基於 I P S e c 隧道、T L S （傳輸層安全性）或 D T L S （資料包傳輸層安全性）的。在該情況下，e N B 9 0 2 與 S M E 9 0 4 之間的 S 1 A P 訊息使用透明容器隧道穿越 H M M E 9 0 6 。

【 0 0 9 1 】 除了關於圖 4 - 6 描述的控制平面安全性，可以在使用者平面處實現額外的安全性以使客戶端設備與 S M E 之間的通訊安全。圖 1 4 是根據本案內容的態樣圖示

具有擴展的使用者平面安全性的H M M E控制平面模型的圖。擴展的使用者平面安全性可以被實現在圖4-6中示出的所有三個H M M E控制平面模型中，或者其他適當的H M M E控制平面模型中。例如，客戶端設備1002（例如，U E）可以使用多個使用者平面（U P）安全性上下文1004來執行與多個封包資料閘道（P - G W）的額外的認證。除了由E S M上下文1006和安全性上下文1008提供的那些之外，U P安全性上下文1004允許服務提供者向客戶端設備1002與該服務提供者的網路之間的訊息或通訊提供額外的安全層。此外，U P安全性可以由服務提供者來控制和維護，使得訊息或通訊的資訊和內容可以免遭連線性提供者的網路（例如，R A N 1010和H M M E）的破壞。

【0092】 在本案內容的態樣中，第一P - G W 1014、第二P - G W 1016和第三P - G W 1018分別提供到第一服務網路1020、第二服務網路1022和第三服務網路1024的连接。第一P - G W 1014可以經由基於相應的U P安全性上下文（例如，U P安全性1）與第一H S S / A A A 1026執行認證程序來檢查客戶端設備1002是否具有針對服務的有效訂閱或憑證。第二P - G W 1016可以經由基於相應的U P安全性上下文（例如，U P安全性2）與第二H S S / A A A 1028執行認證程序來檢查客戶端設備1002是否具有針對服務的有效訂閱或憑證。類似地，第三P - G W 1018可以經由基於相應的U P安全性上下文（例如，U P安全性3）與第三H S S / A A A 1030執行認證程序

來檢查客戶端設備 1002 是否具有針對服務的有效訂閱或憑證。

【0093】圖 15-17 是根據本案內容的態樣圖示使用存取層安全性上下文的一些示例性 H M M E 使用者平面模型的圖。在這些實例中，每一客戶端設備使用一個 E M M 上下文來與存取網路（R A N）建立單個網路連接或鏈路，同時多個 E S M 上下文和存取層（A S）安全性上下文被用於與不同的服務提供者（服務網路）建立服務連接。E M M 上下文和 E S M 上下文可以使用如上關於圖 7-11 描述的程序來建立。A S 安全性上下文可以被用來使客戶端設備與 R A N 之間的使用者平面通訊安全並且對其進行保護。這些 H M M E 資料平面模型可以與上文在圖 4-6 中描述的 H M M E 控制平面模型或其他適當的控制平面模型一起實現。

【0094】圖 15 圖示可以與圖 4 和 5 中示出的 H M M E 控制平面模型或其他適當的 H M M E 控制平面模型一起實現的第一 H M M E 資料平面模型 1100。在圖 15 中示出的實例中，針對客戶端設備 1102 與 R A N 1104 之間的 U E 到 R A N 資料平面傳輸量，客戶端設備 1102（例如，U E）根據與去往某個服務網路的訊息相對應的 E S M 上下文 1108 決定 A S 安全性上下文 1106。在該實例中，三個 A S 安全性上下文 1106 是從三個 E S M 上下文 1108 獲得的。客戶端設備 1102 已經與第一服務網路 1110 建立了第一 E S M 上下文（E S M 上下文 1）、與第二服務網路 1112 建

立了第二ESM上下文（ESM上下文2）以及與第三服務網路1114建立了第三ESM上下文（ESM上下文3）。第一HMM E資料平面模型1100針對不同的P-GW 1118使用單獨的S-GW 1116。

【0095】對於控制訊息（例如，RRC訊息），客戶端設備1102可以基於AS安全性上下文對該訊息進行加密和完整性保護，並且向訊息添加VESM標籤。對於資料訊息，客戶端設備1102可以基於AS安全性上下文對資料訊息進行加密並且向訊息添加VESM標籤。

【0096】對於RAN到UE的資料平面傳輸量，RAN節點1104（例如，eNB）為要被發送給UE或客戶端設備1102的訊息決定AS安全性上下文。在一個實例中，對於控制訊息（例如，RRC訊息），可以使用從HMM E的ESM安全性上下文獲得的預設的AS安全性上下文（在圖15中未圖示）。在RAN 1104（例如，eNB）處，通信期上下文1120（例如，通信期上下文1、2、3）提供被用來將來自客戶端1102（例如，UE）的封包轉發給S-GW 1116或者反之亦然的資訊。例如，通信期上下文可以包括承載ID、QoS資訊、隧道端點ID等等。S-GW 1116處的通信期上下文類似於RAN 104的彼等通信期上下文。例如，這些上下文可以提供被用來將從P-GW 1118接收的針對客戶端1102的封包轉發給RAN 1104（例如，eNB）並且反之亦然的資訊。

【0097】對於控制訊息（例如，RRC訊息），RAN節點1104可以基於AS安全性上下文對訊息進行加密和完整性保護，並且向訊息添加VESM標籤。對於資料訊息，RAN節點1104可以基於AS安全性上下文對訊息進行加密並且向訊息添加VESM標籤。在一個實例中，可以根據TEID（唯一隧道端點辨識符）和S-GW IP位址來決定VESM標籤。在接收到來自RAN節點1104的訊息時，客戶端設備1102可以決定相應的AS安全性上下文以基於該VESM標籤來驗證該訊息。

【0098】圖16圖示可以與圖6中示出的HMM E控制平面模型或其他適當的HMM E控制平面模型一起實現的第二HMM E資料平面模型1200。在第二HMM E資料平面模型1200中，對於客戶端設備1202與RAN 1204之間的UE到RAN的資料平面傳輸量，客戶端設備1202（例如，UE）決定與去往某個服務網路的訊息相對應的AS安全性上下文1206。在該實例中，從ESM上下文1208獲得三個AS安全性上下文1206。客戶端設備1202已經與第一服務網路1210建立了第一ESM上下文（ESM上下文1）、與第二服務網路1212建立了第二ESM上下文（ESM上下文2）以及與第三服務網路1214建立了第三ESM上下文（ESM上下文3）。第二HMM E資料平面模型1200針對不同的P-GW 1218使用公共的S-GW 1216。第二HMM E資料平面模型1200類似於第一

H M M E 資料平面模型 1 1 0 0，並且為了簡潔將不重複對第二 H M M E 資料平面模型 1 2 0 0 的冗餘的描述。

【 0 0 9 9 】 圖 1 7 圖示可以與圖 6 中示出的 H M M E 控制平面模型或其他適當的 H M M E 控制平面模型一起實現的第三 H M M E 資料平面模型 1 3 0 0。客戶端設備 1 3 0 2 可能已經建立了不同的 E S M 上下文 1 3 0 8，例如，分別針對第一服務網路 1 3 1 0、第二服務網路 1 3 1 2 和第三服務網路 1 3 1 4 的第一 E S M 上下文、第二 E S M 上下文和第三 E S M 上下文。在該特定實例中，對於 U E 到 R A N 的資料平面傳輸量，客戶端設備 1 3 0 2（例如，U E）可以使用從 E M M 安全性上下文 1 3 0 9 獲得的預設的 A S 安全性上下文 1 3 0 6。在另一個實例中，從 E S M 安全性上下文 1 3 0 8 獲得的 A S 安全性上下文可以被設置為預設的 A S 安全性上下文。對於控制訊息（例如，R R C 訊息），客戶端設備 1 3 0 2 可以基於 A S 安全性上下文對訊息進行加密和完整性保護並且向控制訊息添加 V E S M 標籤。對於資料訊息，客戶端設備 1 3 0 2 可以基於 A S 安全性上下文對資料訊息進行加密並且向訊息添加 V E S M 標籤。

【 0 1 0 0 】 在 R A N 1 3 0 4 處，通信期上下文 1 3 2 0（例如，通信期上下文 1、2、3）提供被用來將來自客戶端 1 3 0 2（例如，U E）的封包轉發給 S - G W 1 3 1 6 或者反之亦然的資訊。例如，通信期上下文可以包括承載 I D、Q o S 資訊、隧道端點 I D 等等。S - G W 1 3 1 6 處的通信期上下文類似於 R A N 1 3 0 4 的那些通信期上下文。例如，這些上

下文可以包括關於如何將從 P - G W 1318 接收的針對客戶端 1302 的封包轉發給 R A N 1304（例如，e N B）和反之亦然的資訊。

【0101】 在上文描述的資料平面模型中，在 R A N 處，U E 上下文包括關於客戶端（例如，U E）的資訊，例如包括通信期上下文、A S 安全性上下文和關於該客戶端的其他狀態。類似地，在 H M M E 處，U E 上下文包括關於該客戶端的資訊，其包括 E M M / E S M 上下文、安全性上下文和其他狀態，例如，I M S I、T M S I 等等。

【0102】 對於 R A N 到 U E 的資料平面傳輸量，R A N 節點 1304（例如，e N B）可以使用由 H M M E 提供的預設的 A S 安全性上下文（在圖 17 中未圖示）。對於控制訊息（例如，R R C 訊息），R A N 節點 1304（例如，e N B）可以基於 A S 安全性對訊息進行加密和完整性保護並且向訊息添加 V E S M 標籤。對於資料訊息，R A N 節點 1304 可以基於 A S 安全性上下文對訊息進行加密並且向訊息添加 V E S M 標籤。例如，V E S M 標籤可以根據 T E I D 和 S - G W I P 位址決定。

【0103】 圖 18 是根據本案內容的態樣圖示示例性使用者平面安全性終止模型 1400 的圖。類似於圖 15 - 17 中描述的那些的客戶端設備 1402 具有與 R A N 1404 建立的單個 E S M 上下文。R A N 1404 被連接到三個 S - G W 1406，該三個 S - G W 1406 被分別連接到不同的封包資料閘道（P - G W）1408。P - G W 1408 之每一者 P - G W 提供到

相應的服務網路 1410 的存取。E M M 上下文和多個 E S M 上下文可以使用上文關於圖 7-11 描述的程序來建立。在該實例中，使用者平面安全性（U P 安全性）終止在封包資料閘道 1408（P - G W 1、P - G W 2、P - G W 3）處。該使用者平面安全性終止模型可以被用在圖 15-17 中示出的資料平面模型中。U P 安全性使得服務提供者能夠保護來自存取網路（例如，R A N 1404）的使用者資料傳輸量。在本案內容的各個態樣中，A S 安全性上下文可以被用來保護客戶端設備與 R A N 之間的資料無線電承載（D R B）和訊號傳遞無線電承載（S R B）二者，並且 U P 安全性是與 D R B 保護分開應用的。

【0104】圖 19 是根據本案內容的態樣圖示在客戶端設備處可操作以建立多個同時的或併發的服務上下文的示例性方法 1500 的流程圖。方法 1500 可以在圖 1、2、4-8、10、11 及 / 或 14-18 中的任何一個中示出的客戶端設備處執行。在方塊 1502 處，客戶端設備基於第一憑證與連線性網路建立無線鏈路或連接。在方塊 1504 處，客戶端設備建立與連接相對應的連接上下文。例如，客戶端設備（U E）可以使用連線性憑證附著到存取網路（例如，R A N）並且利用 H M M E（例如，圖 4-6 的 H M M E）建立到 R A N 的單個連接。在一些實例中，H M M E 可以常駐在核心網路中。此時，單個 E M M 上下文或連線性被建立。在一個實例中，客戶端設備可以利用無線電鏈路建立模組

210 和無線網路通訊介面204（參見圖2）來建立無線鏈路和連線性上下文。

【0105】在方塊1506處，客戶端設備辨識與連線性網路相關聯的一或多個服務網路。例如，客戶端設備可以發送去往一或多個服務網路的第一訊息，並且其中第一訊息被封裝在去往存取網路的網路節點（例如，HMM E）的第二訊息中。當一個訊息被定址到所去往的網路的具體實體（例如，服務網路的HMM E或SME）時，該訊息是去往某個網路的。例如，服務網路可以是圖4-6和14-17中示出的服務網路。客戶端設備可以使用服務上下文建立模組212（參見圖2）執行類似於圖7、8、10和11中示出的那些的程序以辨識服務網路。

【0106】在方塊1508處，客戶端設備使用所建立的無線鏈路或連接與服務網路建立一或多個服務連接，其中該一或多個服務連接是使用各自的第二憑證建立的。在方塊1510處，客戶端設備建立分別與服務連接相對應的一或多個服務上下文。服務上下文可以包括不同的安全性上下文。安全性上下文之每一者安全性上下文包括NAS安全性上下文和AS安全性上下文，並且NAS安全性上下文和AS安全性上下文二者與相同的第二憑證相對應。例如，服務上下文可以是圖4-6和14-17中描述的ESM上下文，並且安全性上下文可以是圖4-6和14-17中描述的那些安全性上下文。客戶端設備可以使用服務上下文建立模組212執行類似於圖7、8、10和11中示出的那些的程序

以建立服務連接和上下文。服務連接之每一者服務連接可以利用基於相應的 A S 安全性上下文的單獨的金鑰來保護，並且由相應的 V E S M 標籤來區分。

【0107】圖20是根據本案內容的態樣圖示方法1500的額外的程序的流程圖。在方塊1512處，客戶端設備可以利用複數個使用者平面（U P）安全性上下文來保護從分別與一或多個服務網路相關聯的複數個封包資料閘道（P - G W）接收的或向其發送的封包。例如，P - G W可以是圖4-8、10、11和14-18中的任何一個中示出的P - G W。

【0108】圖21是根據本案內容的態樣圖示在連線性網路的網路節點處可操作的示例性方法1600的流程圖。方法1600可以在圖1、3、4-8和10-18中的任何一個中示出的網路節點（例如，H M M E）處執行。在方塊1602處，連線性網路的網路節點基於連線性憑證與客戶端設備建立無線鏈路或第一連接。在方塊1604處，網路節點建立與第一連接相對應的連線性上下文。例如，網路節點可以是H M M E（例如，在圖4-14中示出的H M M E），該H M M E接收來自客戶端設備（U E）的第一附著請求以使用連線性憑證與該客戶端設備建立單個連接和相應的E M M上下文。網路節點可以利用無線電鏈路建立模組310和網路通訊介面304和H M M E模組312，使用圖7-11中描述的程序與客戶端設備（參見圖3）建立單個鏈路和E M M上下文。

【0109】 在已經與客戶端設備建立了單個無線鏈路之後，在方塊1606處，網路節點可以接收來自客戶端設備的針對與和連線性網路相關聯的一或多個服務網路建立連接的請求。例如，服務網路可以是圖4-6和14-18中示出的服務網路或提供者。請求可以包括針對使用現有的無線鏈路或連線性與服務網路或提供者中的一或多個建立單獨的ESM上下文的第二附著請求。ESM上下文之每一者ESM上下文可以與不同的安全性上下文相對應。該網路節點可以使用網路通訊介面304（參見圖3）接收來自該客戶端設備的該請求。

【0110】 在方塊1608處，網路節點使用網路節點作為代理，為客戶端設備分別建立與服務網路的一或多個第二連接。在一個實例中，網路節點可以利用SME模組314來使用圖7-11中描述的程序建立第二連接和相應的上下文。

【0111】 圖22是根據本案內容的態樣圖示方法1600的額外的程序的流程圖。在方塊1610處，網路節點可以接收來自該客戶端設備的訊息，其中訊息封裝去往服務網路的另一個訊息。例如，訊息可以是圖8和11中示出的NAS封裝訊息。

【0112】 圖23是根據本案內容的態樣圖示在服務網路的網路節點處可操作的示例性方法1700的流程圖。方法1700可以在圖1、3、4-8和10-18中的任何一個中示出的網路節點（例如，SME）處執行。在方塊1702處，網

路節點接收來自客戶端設備的針對建立連接的請求。例如，SME可以使用其網路通訊介面304（參見圖3）來接收請求。在方塊1704處，網路節點經由連線性網路的網路節點（例如，HME）與客戶端設備建立連接。例如，網路節點可以使用服務管理實體模組/電路/功能單元314來建立連接。在方塊1706處，網路節點建立與連接相對應的服務上下文，其中服務上下文與安全性上下文相關聯。例如，服務管理實體模組/電路/功能單元314可以被SME指令318配置為建立服務上下文334（參見圖3）。

【0113】 應當理解的是，揭示的程序中的步驟的具體順序或層次是對示例性方法的說明。根據設計偏好，應當理解的是可以重新排列程序中的步驟的具體順序或層次。所附方法請求項以作為例子的順序呈現各個步驟的元素，並非意指被限定到所呈現的具體順序或層次。

【符號說明】

【0114】

- 101 無線電鏈路
- 102 客戶端設備
- 104 服務提供者
- 106 供應功能單元
- 108 服務上下文
- 110 服務上下文
- 112 服務上下文
- 114 服務連接

- 1 1 6 服務連接
- 1 1 8 服務連接
- 1 2 0 R A N
- 1 2 2 連 線 性 上 下 文
- 1 2 4 主 M M E ( H M M E )
- 1 2 6 E M M / E S M 上 下 文
- 1 2 8 S M E
- 1 3 0 S M E
- 1 3 2 服 務 閘 道 ( S - G W )
- 1 3 4 服 務 閘 道 ( S - G W )
- 1 3 6 E S M 上 下 文
- 1 3 8 E S M 上 下 文
- 1 4 0 A A A 伺 服 器
- 1 4 2 A A A 伺 服 器
- 1 4 4 歸 屬 授 權 、 認 證 和 計 費 ( H - A A A ) 伺 服 器
- 2 0 2 客 戶 端 設 備
- 2 0 4 無 線 網 路 通 訊 介 面
- 2 0 6 處 理 器
- 2 0 8 記 憶 體 / 儲 存
- 2 1 0 無 線 電 鏈 路 建 立 模 組 / 電 路 / 功 能 單 元
- 2 1 2 服 務 上 下 文 建 立 模 組 / 電 路 / 功 能 單 元
- 2 1 3 使 用 者 平 面 ( U P ) 安 全 性 上 下 文 建 立 模 組 / 電 路 / 功  
能 單 元
- 2 1 6 無 線 電 鏈 路 建 立 指 令

- 2 1 8 服務上下文建立指令
- 2 1 9 安全性上下文建立指令
- 2 2 6 接收器模組 / 電路 / 功能單元
- 2 2 8 發射器模組 / 電路 / 功能單元
- 2 3 0 天線模組 / 電路 / 功能單元
- 2 3 2 連線性上下文
- 2 3 4 服務上下文
- 2 3 5 安全性上下文
- 3 0 2 網路節點
- 3 0 4 網路通訊介面
- 3 0 6 處理器
- 3 0 8 記憶體 / 儲存
- 3 1 0 無線電鏈路建立模組
- 3 1 2 H M M E 模組
- 3 1 4 S M E 模組
- 3 1 6 無線電鏈路建立指令
- 3 1 8 H M M E / S M E 指令
- 3 2 6 接收器模組 / 電路 / 功能單元
- 3 2 8 發射器模組 / 電路 / 功能單元
- 3 3 0 天線模組 / 電路 / 功能單元
- 3 3 2 儲存連線性上下文（或憑證）
- 3 3 4 服務上下文（或憑證）
- 3 3 5 安全性上下文
- 4 0 2 客戶端設備

- 4 0 3   R A N
- 4 0 4   E M M 上 下 文
- 4 0 6   H M M E
- 4 0 7   A A A 伺 服 器
- 4 0 8   E S M 上 下 文
- 4 1 0   安 全 性 上 下 文
- 4 1 2   第 二 S M E
- 4 1 3   A A A 伺 服 器
- 4 1 4   S M E
- 4 1 5   A A A 伺 服 器
- 4 1 8   第 一 服 務 / 封 包 資 料 閘 道 ( S / P   G W )
- 4 2 0   第 一 服 務 網 路
- 4 2 2   第 二 S / P   G W
- 4 2 4   第 二 服 務 網 路
- 4 2 6   第 三 S / P   G W
- 4 2 8   第 三 服 務 網 路
- 4 3 0   無 線 電 鏈 路
- 4 3 1   服 務 閘 道 ( S - G W )
- 4 3 2   P - G W
- 4 3 4   P - G W
- 4 3 6   P - G W
- 5 0 0   撥 叫 流 程 圖
- 5 0 2   U E
- 5 0 4   e N B

- 5 0 6   H M M E
- 5 0 8   S M E
- 5 1 0   服 務 閘 道 ( S - G W )
- 5 1 2   第 一 封 包 資 料 閘 道 ( P - G W )
- 5 1 4   第 二 P - G W
- 5 1 6   第 一 歸 屬 用 戶 伺 服 器 ( H S S )
- 5 1 8   第 二 H S S
- 5 2 0   附 著 請 求
- 5 2 2   初 始 U E 訊 息
- 5 2 4   進 化 型 封 包 系 統 ( E P S ) 認 證 和 金 鑰 協 商 ( A K A )  
程 序
- 5 2 6   N A S 安 全 性 模 式 命 令 ( S M C ) 訊 息
- 5 2 8   建 立 通 信 期 請 求
- 5 2 9   建 立 通 信 期 請 求
- 5 3 0   建 立 通 信 期 回 應 訊 息
- 5 3 2   初 始 上 下 文 建 立 請 求 訊 息
- 5 3 4   R R C 連 接 重 新 配 置 訊 息
- 5 3 6   R R C 連 接 重 新 配 置 完 成 訊 息
- 5 3 8   初 始 建 立 上 下 文 回 應 訊 息
- 5 4 0   服 務 註 冊 訊 息
- 5 4 2   初 始 U E 訊 息
- 5 4 4   E P S - A K A 程 序
- 5 4 6   N A S 安 全 性 模 式 命 令 ( S M C ) 訊 息
- 5 4 8   建 立 通 信 期 請 求

- 5 5 0 建立通信期回應訊息
- 5 5 2 初始上下文建立請求訊息
- 5 5 4 初始上下文建立請求訊息
- 5 5 6 R R C 連接重新配置訊息
- 5 5 8 R R C 連接重新配置完成訊息
- 5 6 0 初始建立上下文回應訊息
- 5 6 2 初始建立上下文回應訊息
- 6 0 0 N A S 訊息
- 6 0 2 S M E I D
- 6 0 4 內部 N A S 訊息
- 6 0 6 U E I D
- 7 0 0 流程圖
- 7 0 2 客戶端設備 ( U E )
- 7 0 4 e N B
- 7 0 6 H M M E
- 7 0 8 S M E
- 7 1 0 S - G W
- 7 1 2 第一 P - G W
- 7 1 4 第二 P - G W
- 7 1 6 第一 H S S
- 7 1 8 第二 H S S
- 7 2 0 服務註冊訊息
- 7 2 2 初始 U E 訊息
- 7 2 4 E P S - A K A 程序

- 7 2 6 N A S 安 全 性 模 式 命 令 ( S M C ) 訊 息
- 7 2 8 建 立 通 信 期 請 求
- 7 3 0 建 立 通 信 期 回 應 訊 息
- 7 3 2 初 始 上 下 文 建 立 請 求 訊 息
- 7 3 4 R R C 連 接 重 新 配 置 訊 息
- 7 3 6 R R C 連 接 重 新 配 置 完 成 訊 息
- 7 3 8 初 始 上 下 文 建 立 回 應 訊 息
- 7 4 0 初 始 上 下 文 建 立 回 應 訊 息
- 8 0 2 e N B
- 8 0 4 S M E
- 8 0 6 H M M E
- 9 0 2 e N B
- 9 0 4 S M E
- 9 0 6 H M M E
- 9 0 8 安 全 通 道
- 1 0 0 2 客 戶 端 設 備
- 1 0 0 4 U P 安 全 性 上 下 文
- 1 0 0 6 E S M 上 下 文
- 1 0 0 8 安 全 性 上 下 文
- 1 0 1 0 R A N
- 1 0 1 4 第 一 P - G W
- 1 0 1 6 第 二 P - G W
- 1 0 1 8 第 三 P - G W
- 1 0 2 0 第 一 服 務 網 路

- 1 0 2 2 第二服務網路
- 1 0 2 4 第三服務網路
- 1 0 2 6 第一 H S S / A A A
- 1 0 2 8 第二 H S S / A A A
- 1 0 3 0 第三 H S S / A A A
- 1 1 0 0 第一 H M M E 資料平面模型
- 1 1 0 2 客戶端設備
- 1 1 0 4 R A N
- 1 1 0 6 A S 安全性上下文
- 1 1 0 8 E S M 上下文
- 1 1 1 0 第一服務網路
- 1 1 1 2 第二服務網路
- 1 1 1 4 第三服務網路
- 1 1 1 6 S - G W
- 1 1 1 8 P - G W
- 1 1 2 0 通信期上下文
- 1 2 0 0 第二 H M M E 資料平面模型
- 1 2 0 2 客戶端設備
- 1 2 0 4 R A N
- 1 2 0 6 A S 安全性上下文
- 1 2 0 8 E S M 上下文
- 1 2 1 0 第一服務網路
- 1 2 1 2 第二服務網路
- 1 2 1 4 第三服務網路

- 1 2 1 6 S - G W
- 1 2 1 8 P - G W
- 1 3 0 0 第三 H M M E 資 料 平 面 模 型
- 1 3 0 2 客 戶 端 設 備
- 1 3 0 4 R A N
- 1 3 0 6 A S 安 全 性
- 1 3 0 8 E S M 上 下 文
- 1 3 0 9 E M M 安 全 性 上 下 文
- 1 3 1 0 第 一 服 務 網 路
- 1 3 1 2 第 二 服 務 網 路
- 1 3 1 4 第 三 服 務 網 路
- 1 3 1 6 S - G W
- 1 3 1 8 P - G W
- 1 3 2 0 通 信 期 上 下 文
- 1 4 0 0 使 用 者 平 面 安 全 性 終 止 模 型
- 1 4 0 2 客 戶 端 設 備
- 1 4 0 4 R A N
- 1 4 0 6 S - G W
- 1 4 0 8 P - G W
- 1 4 1 0 服 務 網 路
- 1 5 0 0 方 法
- 1 5 0 2 方 塊
- 1 5 0 4 方 塊
- 1 5 0 6 方 塊

- 1 5 0 8 方 塊
- 1 5 1 0 方 塊
- 1 5 1 2 方 塊
- 1 6 0 0 方 法
- 1 6 0 2 方 塊
- 1 6 0 4 方 塊
- 1 6 0 6 方 塊
- 1 6 0 8 方 塊
- 1 6 1 0 方 塊
- 1 7 0 0 方 法
- 1 7 0 2 方 塊
- 1 7 0 4 方 塊
- 1 7 0 6 方 塊

【生物材料寄存】

【 0 1 1 5 】 國內寄存資訊 (請依寄存機構、日期、號碼順序註記)

無

【 0 1 1 6 】 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

## 【發明申請專利範圍】

【第1項】 一種在一無線通訊網路中操作一客戶端設備的方法，包括以下步驟：

基於一第一憑證來與一連線性網路建立一連線性上下文；

使用與該連線性網路所建立的該連線性上下文來與關聯於該連線性網路的一或多個服務網路建立一或多個服務上下文，其中該一或多個服務上下文是使用一或多個第二憑證來建立的；

其中該一或多個服務上下文分別包括不同的安全性上下文，並且

其中該等安全性上下文之每一個安全性上下文包括一非存取層（NAS）安全性上下文和一存取層（AS）安全性上下文，該NAS安全性上下文和該AS安全性上下文二者與相同的第二憑證相對應。

【第2項】 如請求項1之方法，

其中該NAS安全性上下文被配置為保護該客戶端設備與下列各項中的至少一項之間的控制訊息：一主行動性管理實體（HMM E）或一服務管理實體（SME），並且

其中該AS安全性上下文被配置為保護以下各項中的至少一項：一或多個訊號傳遞無線電承載、一或多

個資料無線電承載、或一或多個訊號傳遞無線電承載和一或多個資料無線電承載的一組合。

【第3項】 如請求項1之方法，其中建立一或多個服務上下文包括發送去往該一或多個服務網路的一訊息，其中該訊息被封裝在去往該連線性網路的一主行動性管理實體（H M M E）的一訊息中。

【第4項】 如請求項1之方法，其中該一或多個服務網路包括至少部分地在該連線性網路中建立的一虛擬網路，並且該一或多個服務網路分別與不同的服務相關聯。

【第5項】 如請求項1之方法，其中該一或多個服務上下文之每一個服務上下文是利用基於相應的該A S安全性上下文的一單獨的金鑰來保護的，並且由一相應的虛擬進化型封包系統（E P S）通信期管理標籤來區分的。

【第6項】 如請求項1之方法，亦包括以下步驟：

使用複數個使用者平面（U P）安全性上下文來保護從複數個封包資料閘道接收的或向其發送的封包，該複數個封包資料閘道分別與該一或多個服務網路相關聯。

【第7項】 如請求項6之方法，其中保護該等封包包括以下各項中的至少一項：

對該等封包進行加密；

對該等封包進行完整性保護；或

對該等封包進行加密和完整性保護。

【第8項】 一種操作一連線性網路的一網路節點的方法，包括以下步驟：

基於一連線性憑證來與一客戶端設備建立一第一連線性上下文；

從該客戶端設備，接收針對與一或多個分別的服務網路建立一或多個服務上下文的一請求；及

使用該網路節點作為一代理，利用一或多個服務憑證為該客戶端設備分別建立與該一或多個服務網路的複數個服務上下文，其中該網路節點包括一主行動性管理實體（H M M E），

其中該複數個服務上下文分別包含不同的安全性上下文，並且

其中該等安全性上下文之每一個安全性上下文包括一非存取層（N A S）安全性上下文和一存取層（A S）安全性上下文，該N A S安全性上下文和該A S安全性上下文二者與相同的服務憑證相對應。

【第9項】 如請求項8之方法，其中該等服務上下文包括IP安全性（I P S e c）隧道。

【第10項】 如請求項8之方法，亦包括接收來自該客戶端設備的一訊息，其中該訊息封裝去往該一或多個服務網路的另一個訊息。

【第11項】 一種操作一服務網路的一網路節點的方法，包括以下步驟：

從一客戶端設備，接收針對基於一第一憑證建立一連線性上下文的一請求；

經由一連線性網路的一網路節點來與該客戶端設備建立該連線性上下文，其中該連線性網路的該網路節點包括一主行動性管理實體（H M M E）；及

基於一服務憑證來建立與該連線性上下文相對應的一服務上下文，其中該服務上下文與一安全性上下文相關聯，

其中該安全性上下文包括一非存取層（N A S）安全性上下文和一存取層（A S）安全性上下文，該N A S安全性上下文和該A S安全性上下文二者與相同的該服務憑證相對應。

【第12項】 如請求項11之方法，其中該服務上下文包括經由該連線性網路的該網路節點的一IP安全性（I P S e c）隧道。

【第13項】 如請求項11之方法，其中該服務上下文包括至少部分地在該連線性網路中建立的一虛擬網路。

【第14項】 如請求項11之方法，其中該服務上下文與一虛擬進化型封包系統（EPS）通信期管理標籤相關聯。

【第15項】 一種在一無線通訊網路中的客戶端設備，包括：

一記憶體，其包括電腦可執行代碼；

一通訊介面，其被配置為與一連線性網路進行通訊；及

一處理器，其被操作地耦合至該記憶體和該通訊介面，

其中該處理器被該電腦可執行代碼配置為：

基於一第一憑證來與一連線性網路建立一連線性上下文；

使用與該連線性網路所建立的該連線性上下文來與關聯於該連線性網路的一或多個服務網路建立一或多個服務上下文，其中該一或多個服務上下文是使用一或多個第二憑證建立的；及

其中該一或多個服務上下文分別包括不同的安全性上下文，並且

其中該等安全性上下文之每一個安全性上下文包括一非存取層（NAS）安全性上下文和一存取層

( A S ) 安全性上下文，該 N A S 安全性上下文和該 A S 安全性上下文二者與相同的第二憑證相對應。

【第 1 6 項】 如請求項 1 5 之客戶端設備，

其中該 N A S 安全性上下文被配置為保護該客戶端設備與下列各項中的至少一項之間的控制訊息：一主行動性管理實體 ( H M M E ) 或一服務管理實體 ( S M E ) ，並且

其中該 A S 安全性上下文被配置為保護以下各項中的至少一項：一或多個訊號傳遞無線電承載、一或多個資料無線電承載、或一或多個訊號傳遞無線電承載和一或多個資料無線電承載的一組合。

【第 1 7 項】 如請求項 1 5 之客戶端設備，其中為了建立該一或多個服務上下文，該處理器亦被配置為發送去往該一或多個服務網路的一訊息，其中該訊息被封裝在去往該連線性網路的一主行動性管理實體 ( H M M E ) 的一訊息中。

【第 1 8 項】 如請求項 1 5 之客戶端設備，其中該一或多個服務網路包括至少部分地在該連線性網路中建立的一虛擬網路，並且該一或多個服務網路分別與不同的服務相關聯。

【第 1 9 項】 如請求項 1 5 之客戶端設備，其中該等服務上下文之每一個服務上下文是利用基於相應的該 A S

安全性上下文的一單獨的金鑰來保護的，並且由一相應的虛擬進化型封包系統（EPS）通信期管理標籤來區分的。

【第20項】 如請求項15之客戶端設備，其中該處理器亦被配置為：

使用複數個使用者平面（UP）安全性上下文來保護從複數個封包資料閘道接收的或向其發送的封包，該複數個封包資料閘道分別與該一或多個服務網路相關聯。

【第21項】 如請求項20之客戶端設備，其中該處理器亦被配置為經由以下各項中的至少一項來保護該等封包：

對該等封包進行加密；

對該等封包進行完整性保護；或

對該等封包進行加密和完整性保護。

【第22項】 一種用於一連線性網路的網路節點，包括：

一記憶體，其包括電腦可執行代碼；

一通訊介面，其被配置為與一客戶端設備進行通訊；及

一處理器，其被操作地耦合到該記憶體和該通訊介面，

其中該處理器被該電腦可執行代碼配置為：

基於一連線性憑證來與該客戶端設備建立一第一連線性上下文；

從該客戶端設備，接收針對與一或多個分別的服務網路建立一或多個服務上下文的一請求；及

使用該網路節點作為一代理，利用一或多個服務憑證為該客戶端設備分別建立與該一或多個服務網路的複數個服務上下文，其中該網路節點包括一主行動性管理實體（H M M E），

其中該複數個服務上下文分別包含不同的安全性上下文，並且

其中該等安全性上下文之每一個安全性上下文包括一非存取層（N A S）安全性上下文和一存取層（A S）安全性上下文，該N A S安全性上下文和該A S安全性上下文二者與相同的服務憑證相對應。

【第23項】 如請求項22之網路節點，其中該等服務上下文包括IP安全性（I P S e c）隧道。

【第24項】 如請求項22之網路節點，其中該處理器亦被配置為接收來自該客戶端設備的一訊息，其中該訊息封裝去往該一或多個服務網路的另一個訊息。

【第25項】 一種用於一服務網路的網路節點，包括：  
一記憶體，其包括電腦可執行代碼；

一通訊介面，其被配置為與一客戶端設備進行通訊；及

一處理器，其被操作地耦合至該記憶體和該通訊介面，

其中該處理器被該代碼配置為：

從該客戶端設備，接收針對基於一第一憑證建立一連線性上下文的一請求；

經由一連線性網路的一網路節點來與該客戶端設備建立該連線性上下文，其中該連線性網路的該網路節點包括一主行動性管理實體（H M M E）；及

基於一服務憑證來建立與該連接相對應的一服務上下文，其中該服務上下文與一安全性上下文相關聯，

其中該安全性上下文包括一非存取層（N A S）安全性上下文和一存取層（A S）安全性上下文，該N A S安全性上下文和該A S安全性上下文二者與相同的該服務憑證相對應。

【第26項】 如請求項25之網路節點，其中該服務上下文包括經由該連線性網路的該網路節點的一IP安全性（I P S e c）隧道。

【第27項】 如請求項25之網路節點，其中該服務上下文包括至少部分地在該連線性網路中建立的一虛擬網路。

【第28項】 如請求項25之網路節點，其中該服務上下文與虛擬進化型封包系統（EPS）通信期管理標籤相關聯。

【發明圖式】

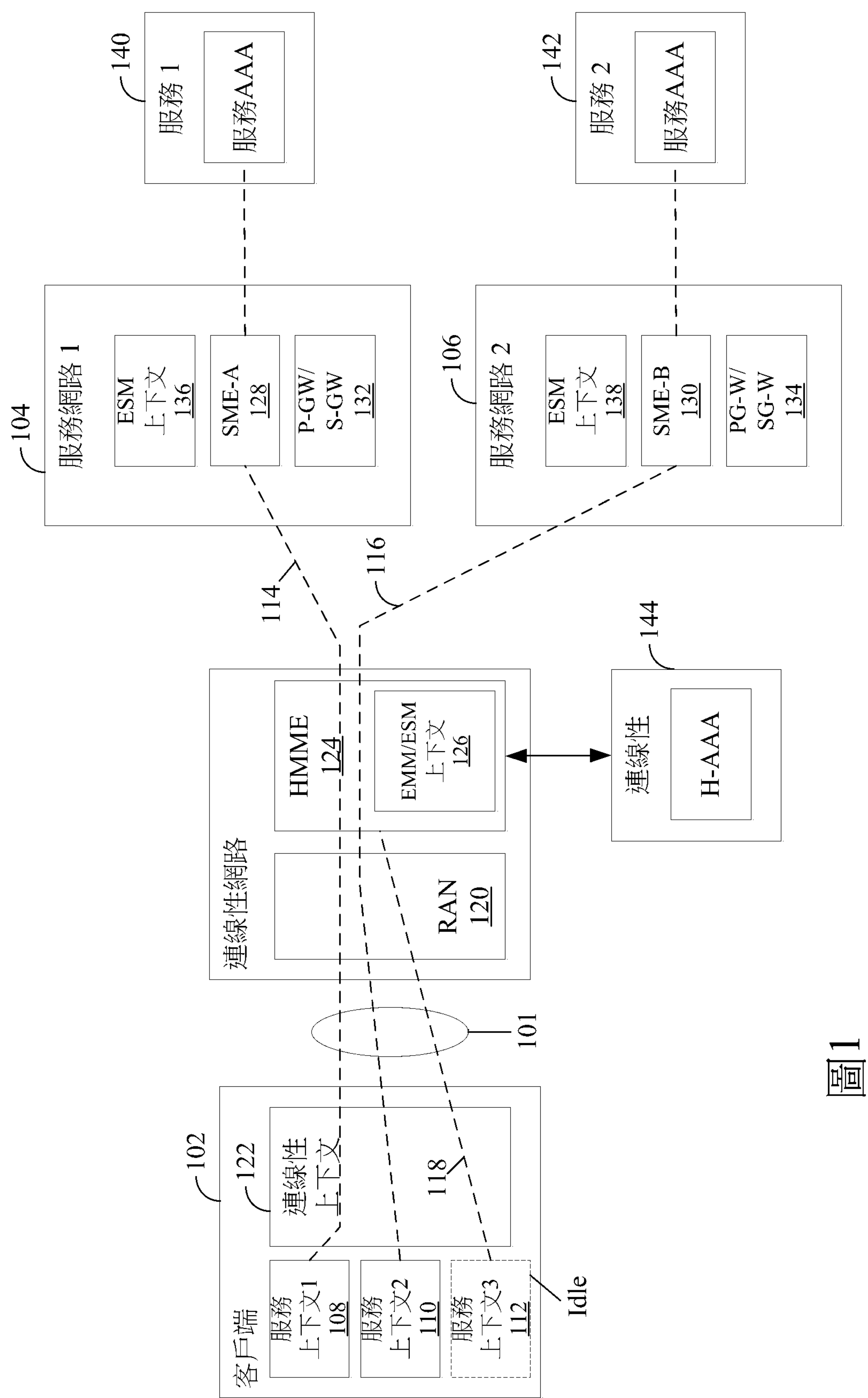


圖1

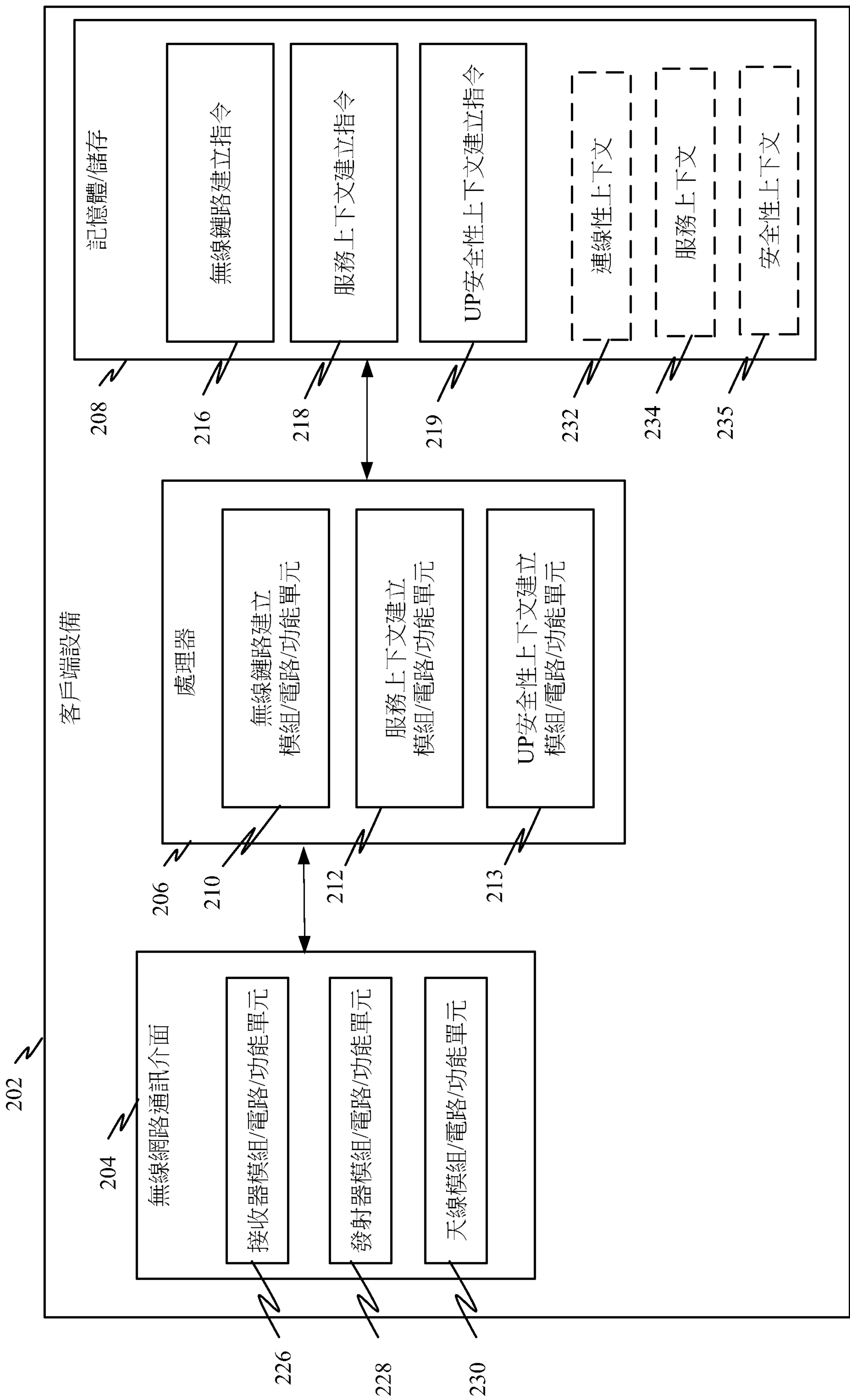


圖2

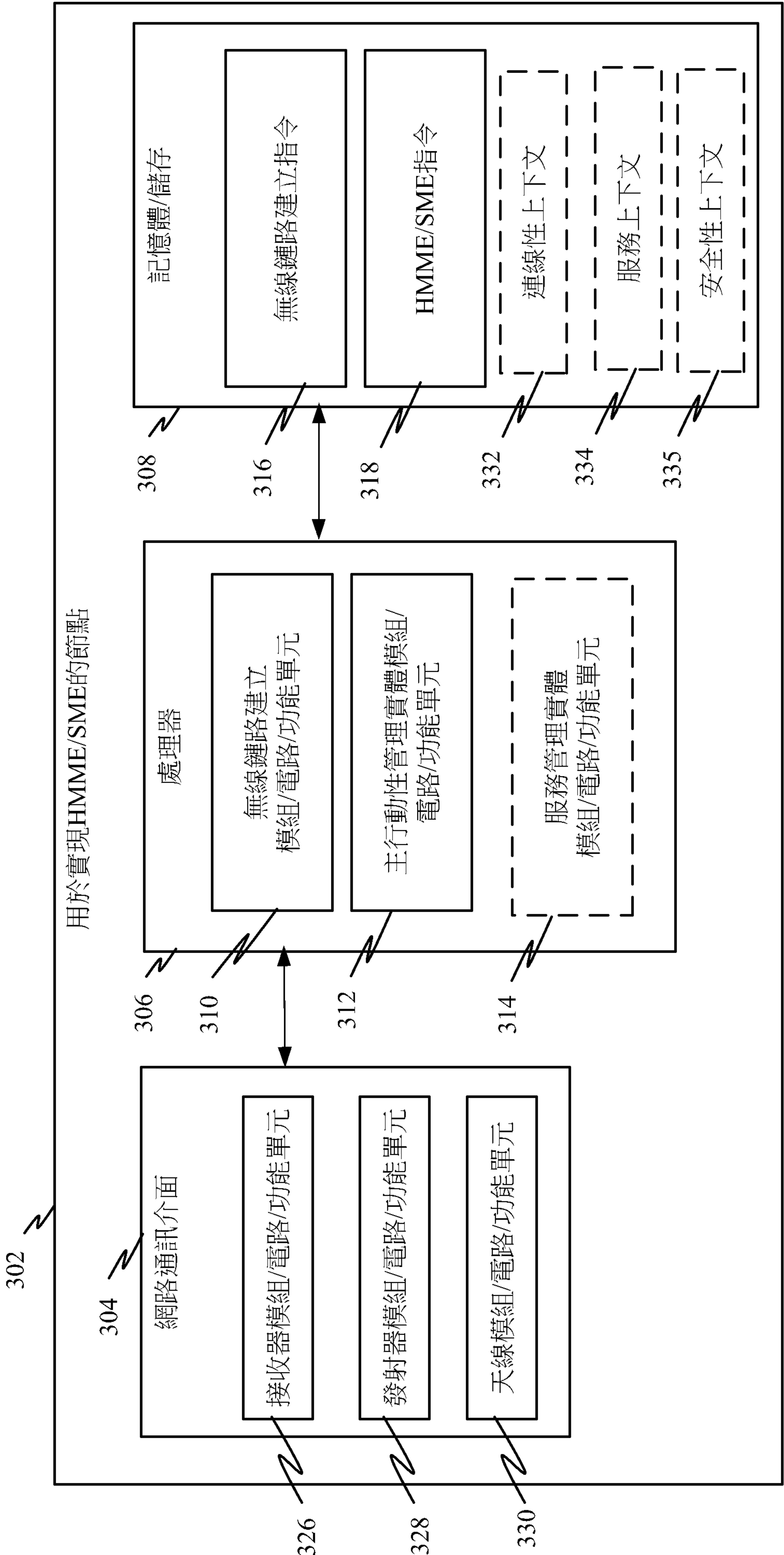


圖3

HMME控制平面模型1

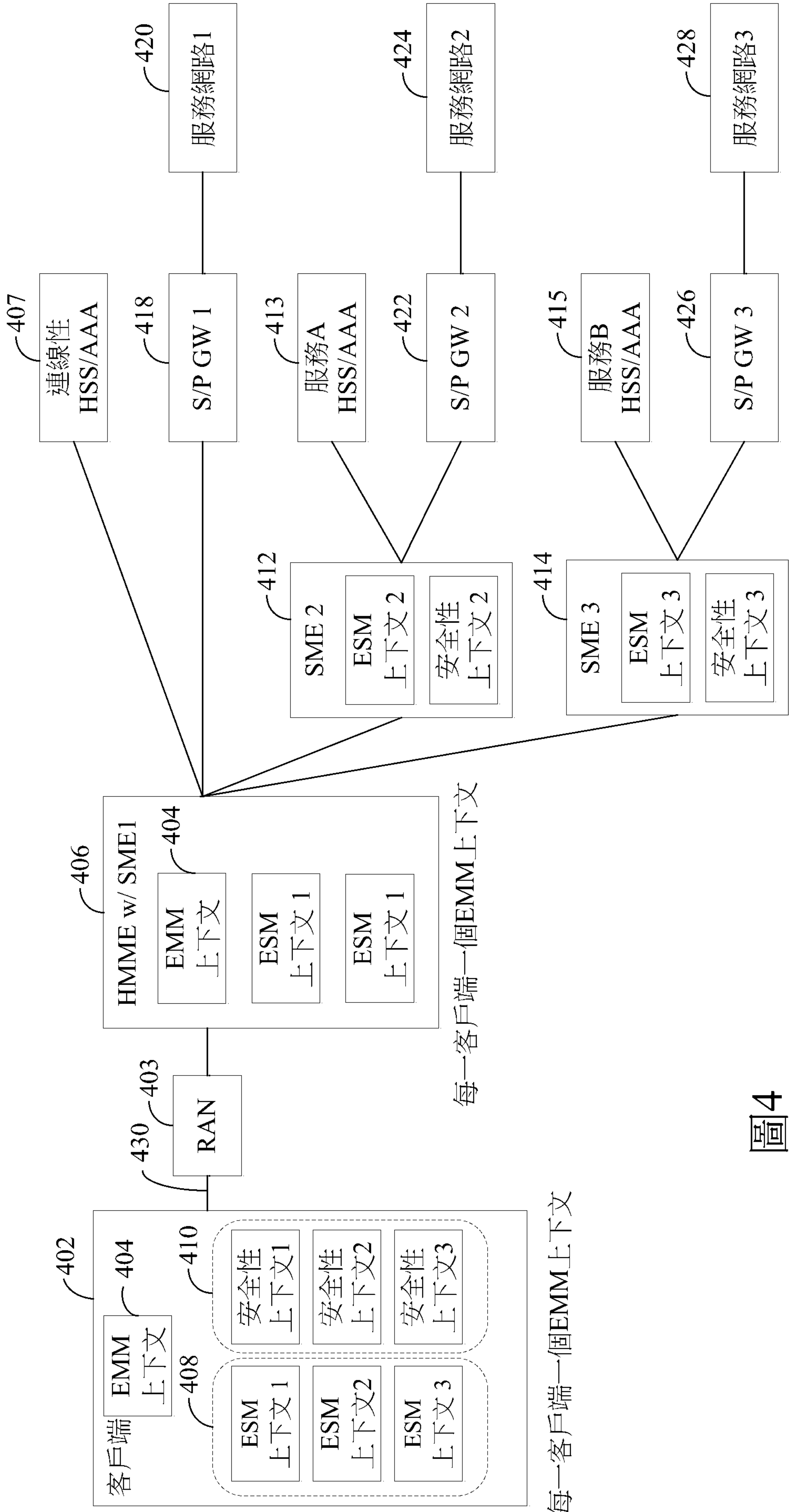


圖4

每一客戶端一個EMM上下文

HMME控制平面模型2

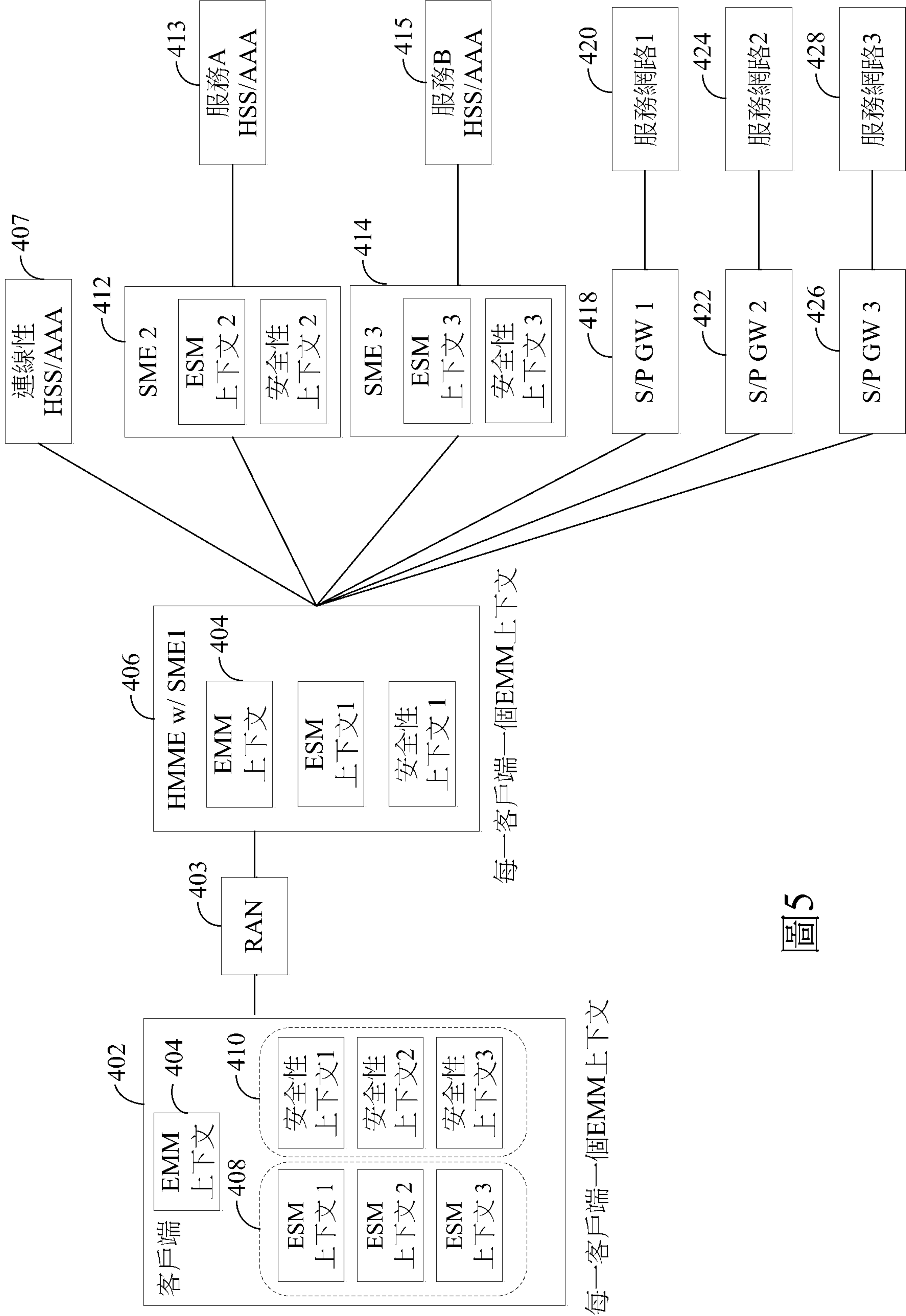


圖5

HMME控制平面模型3

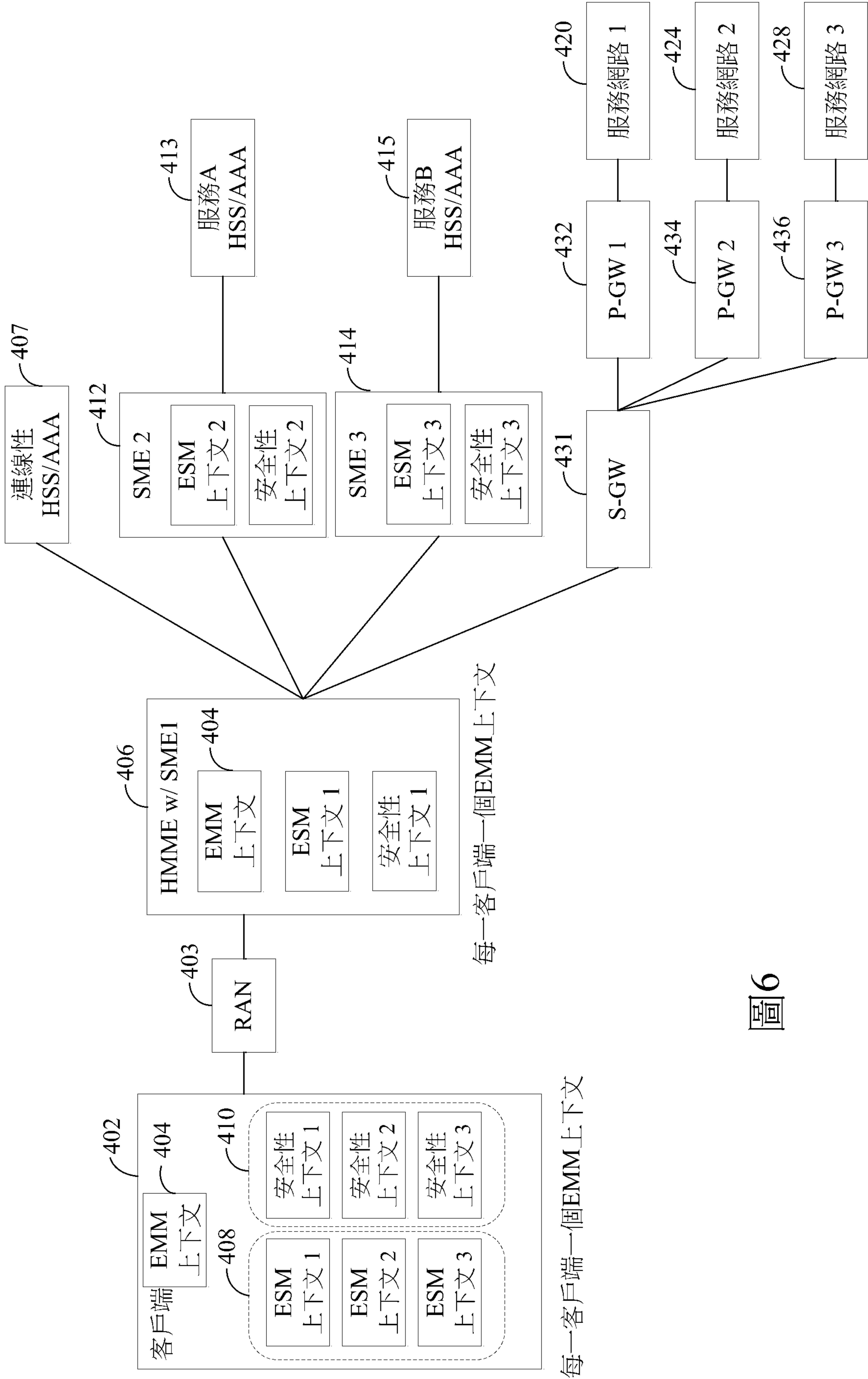


圖6

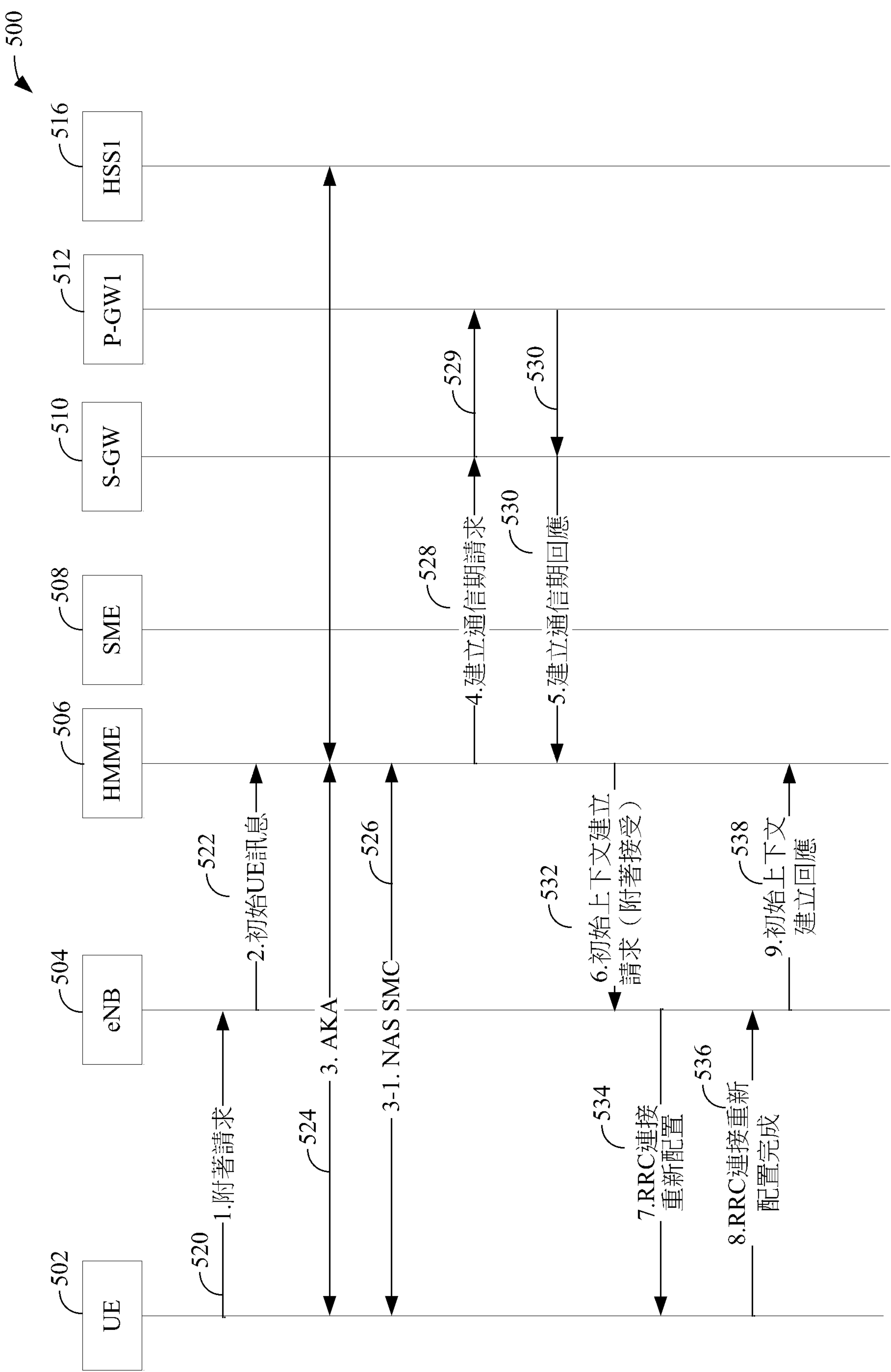


圖7

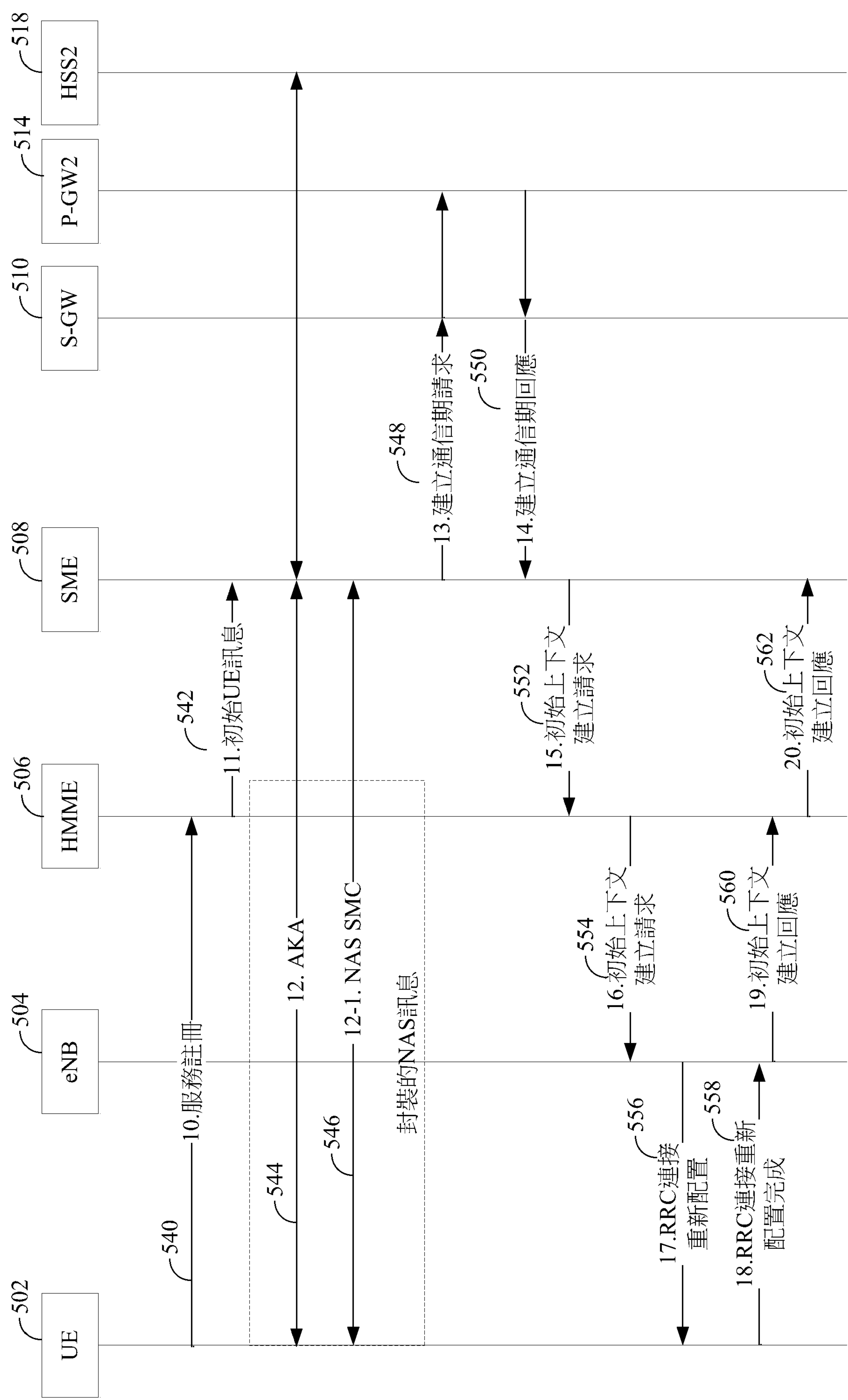


圖8

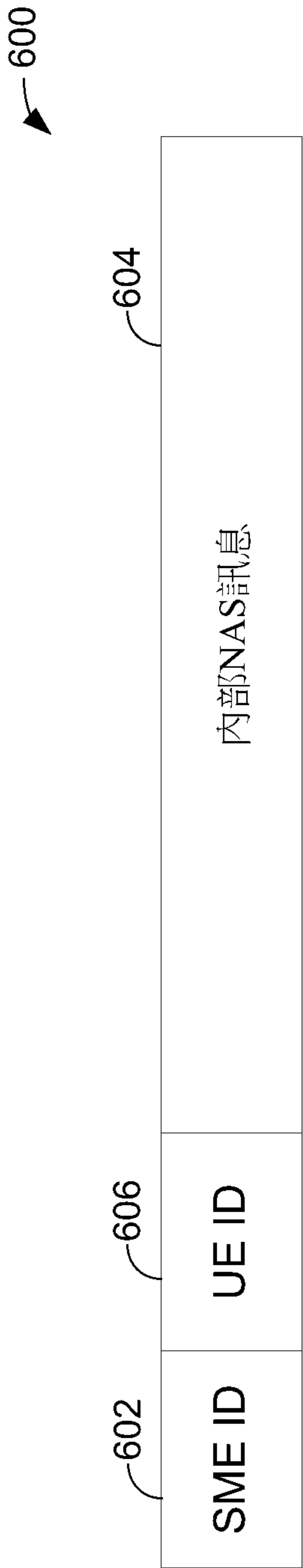


圖9

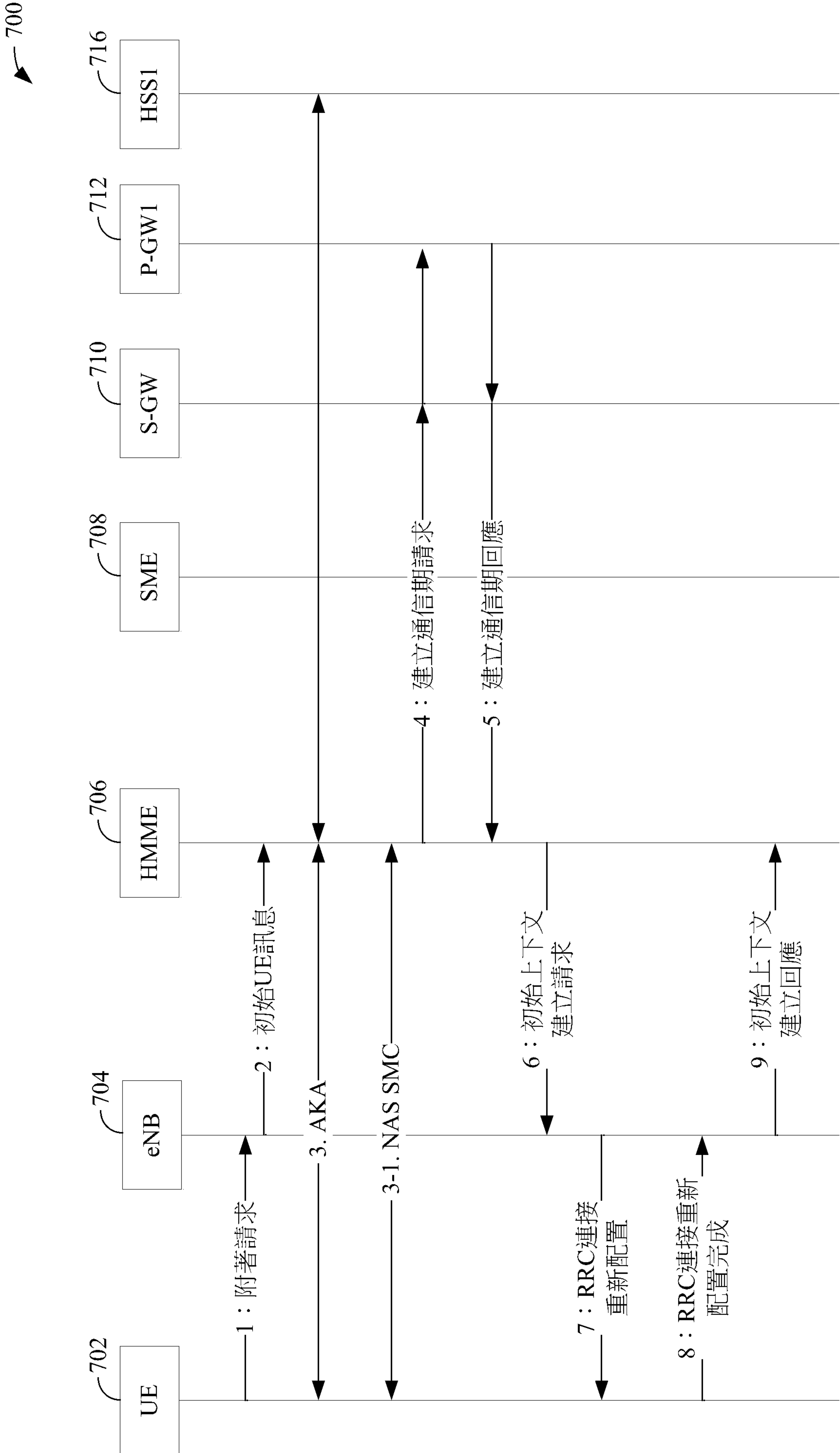


圖10

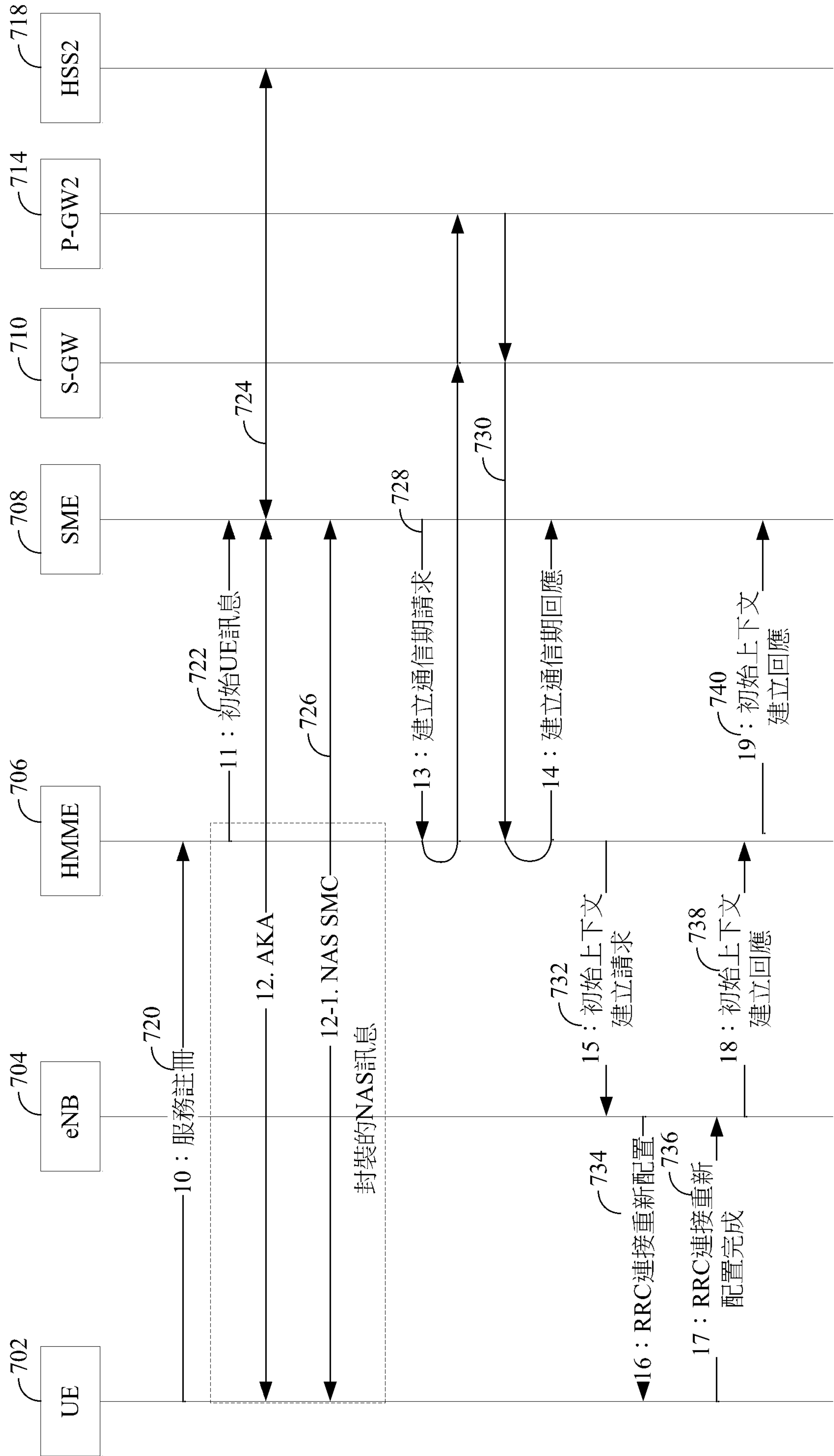


圖11

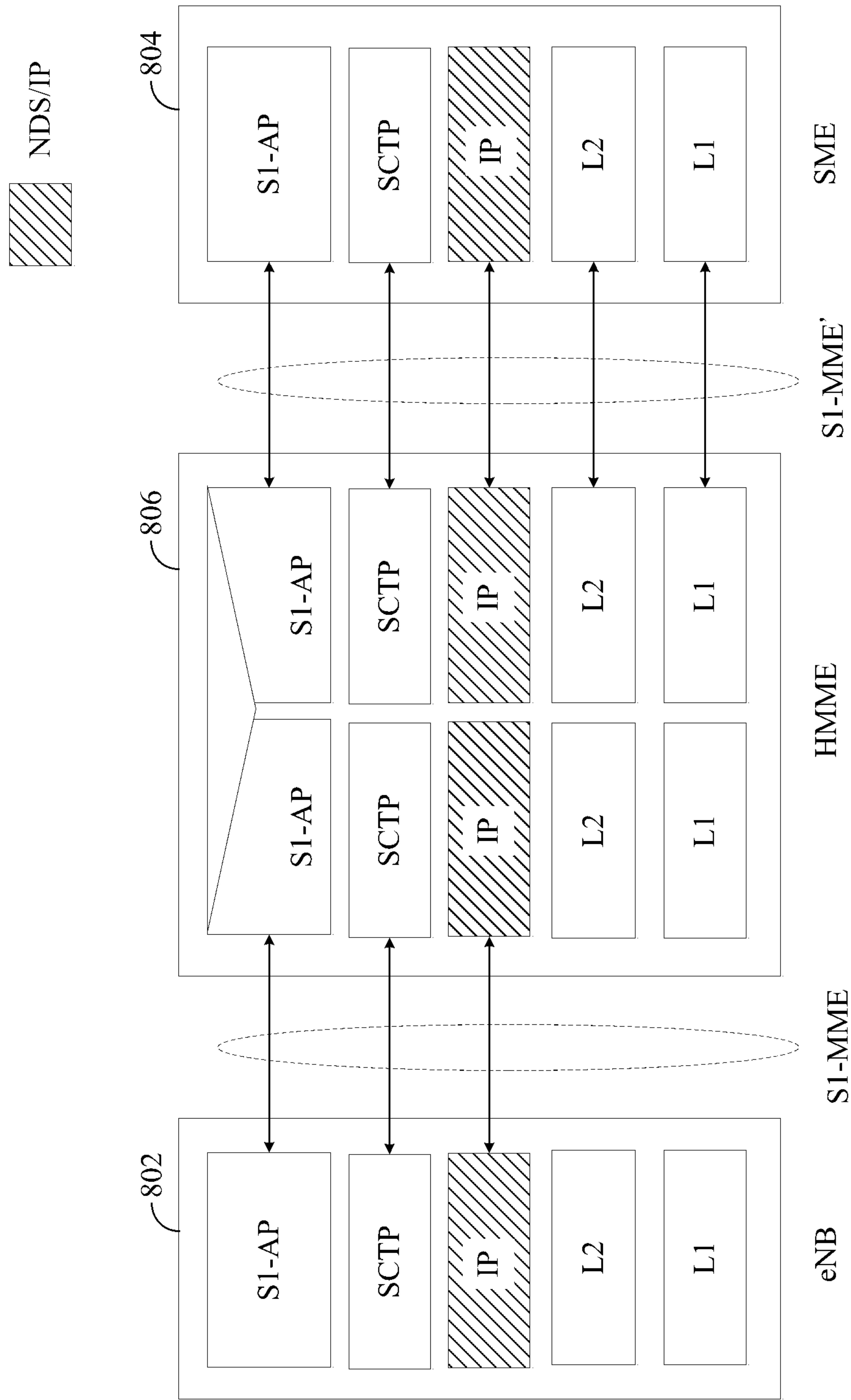


圖12

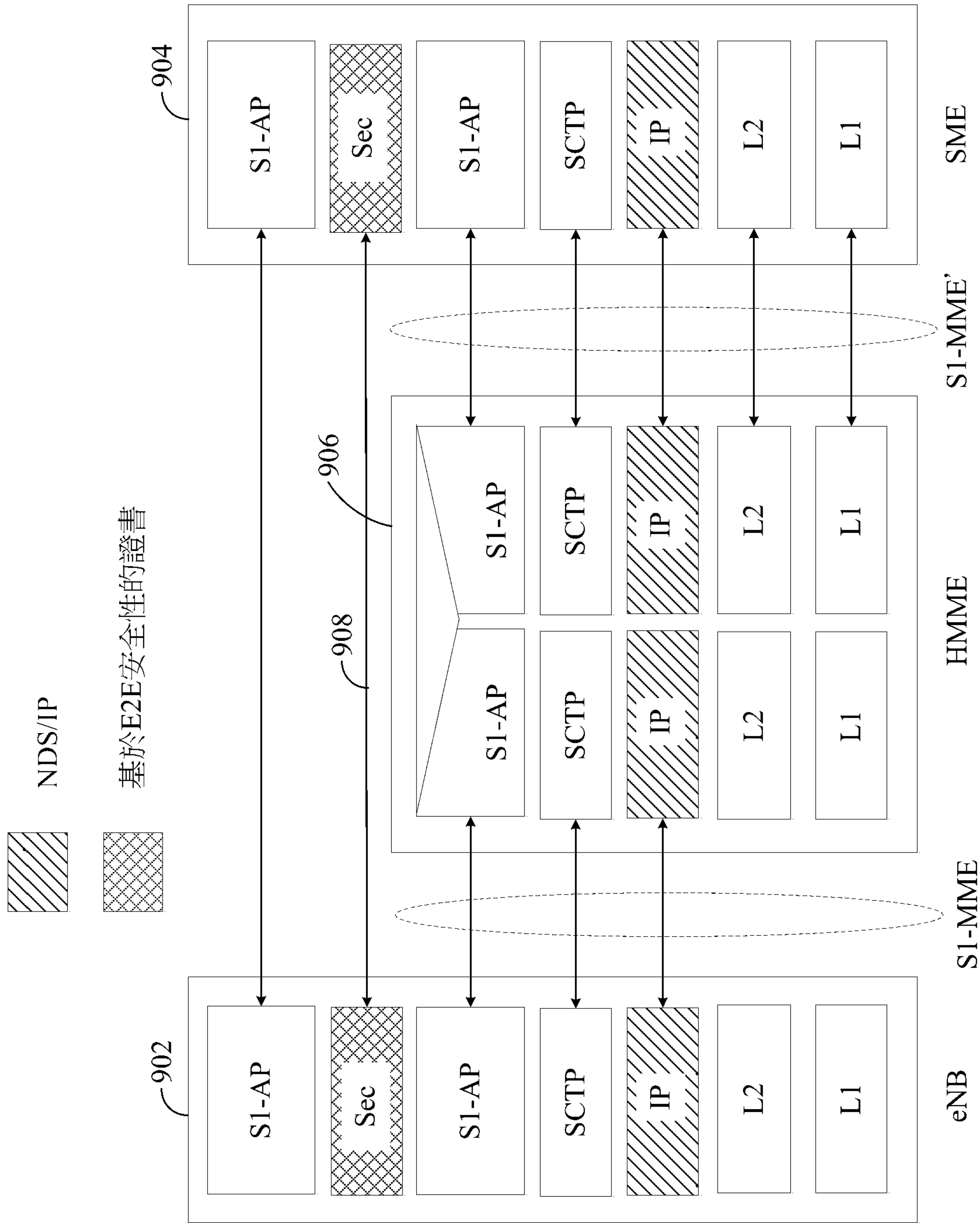


圖13

具有擴展的使用者平面安全性的HMME控制平面模型

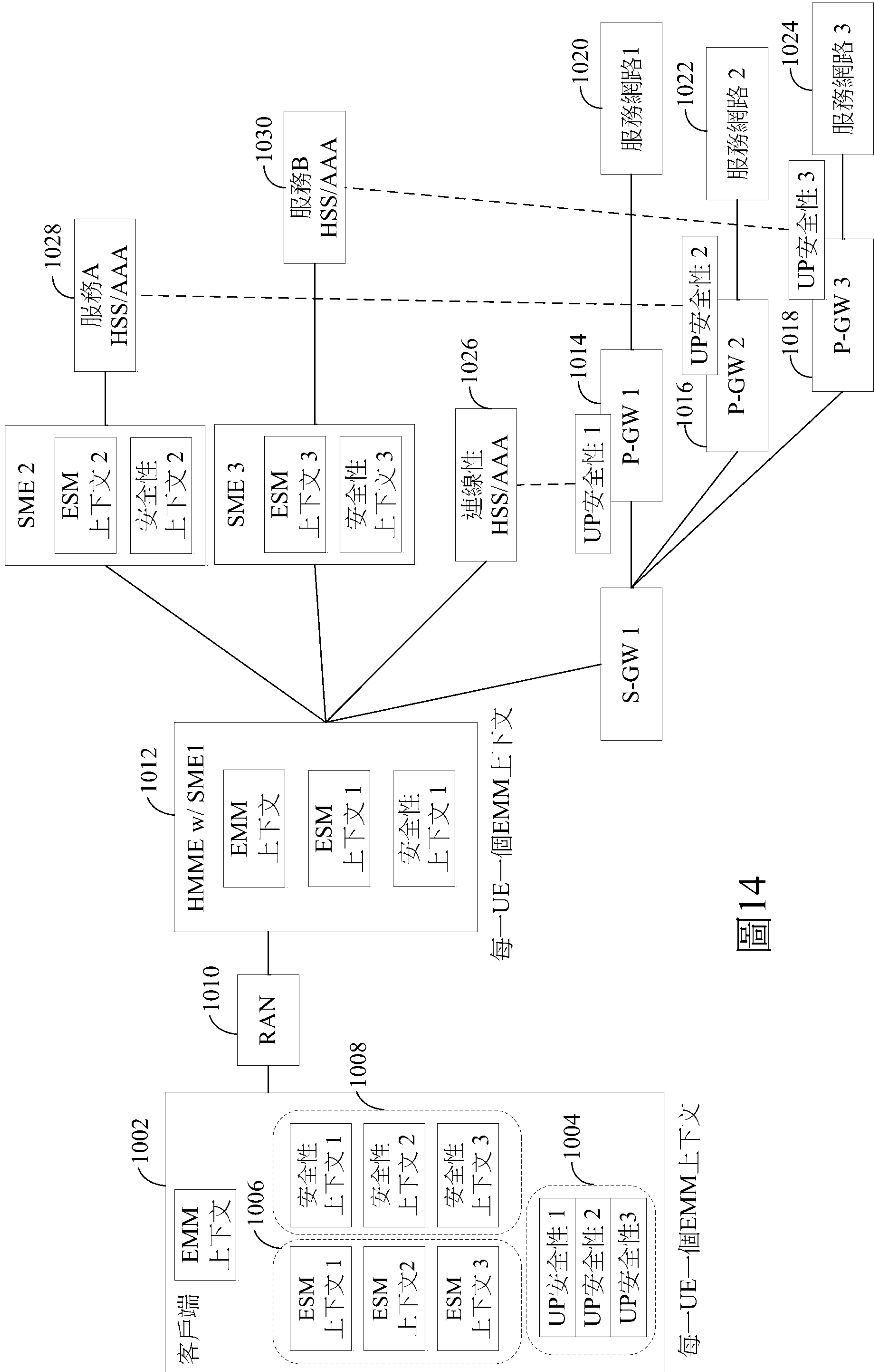


圖14

HMME資料平面模型1

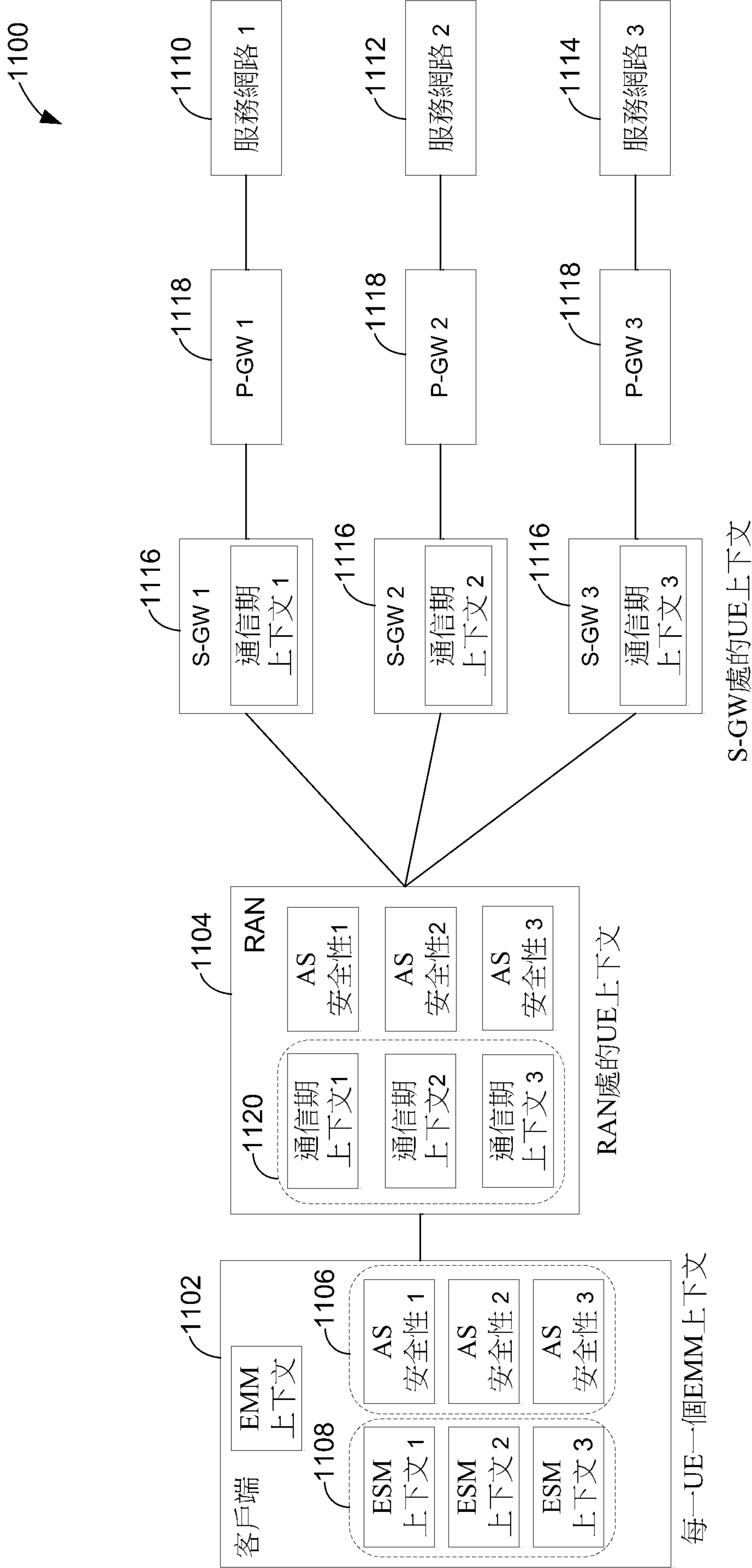


圖15

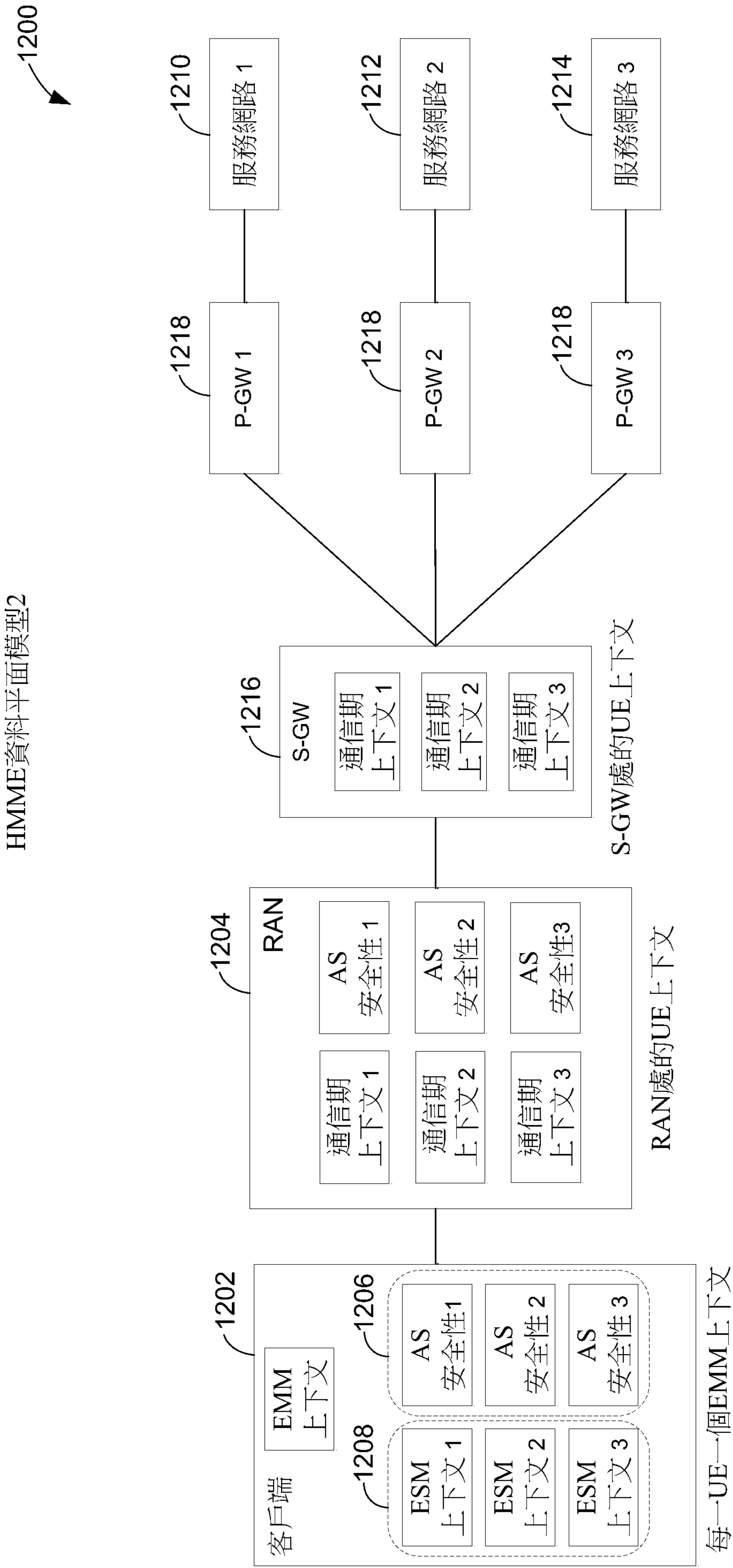


圖16

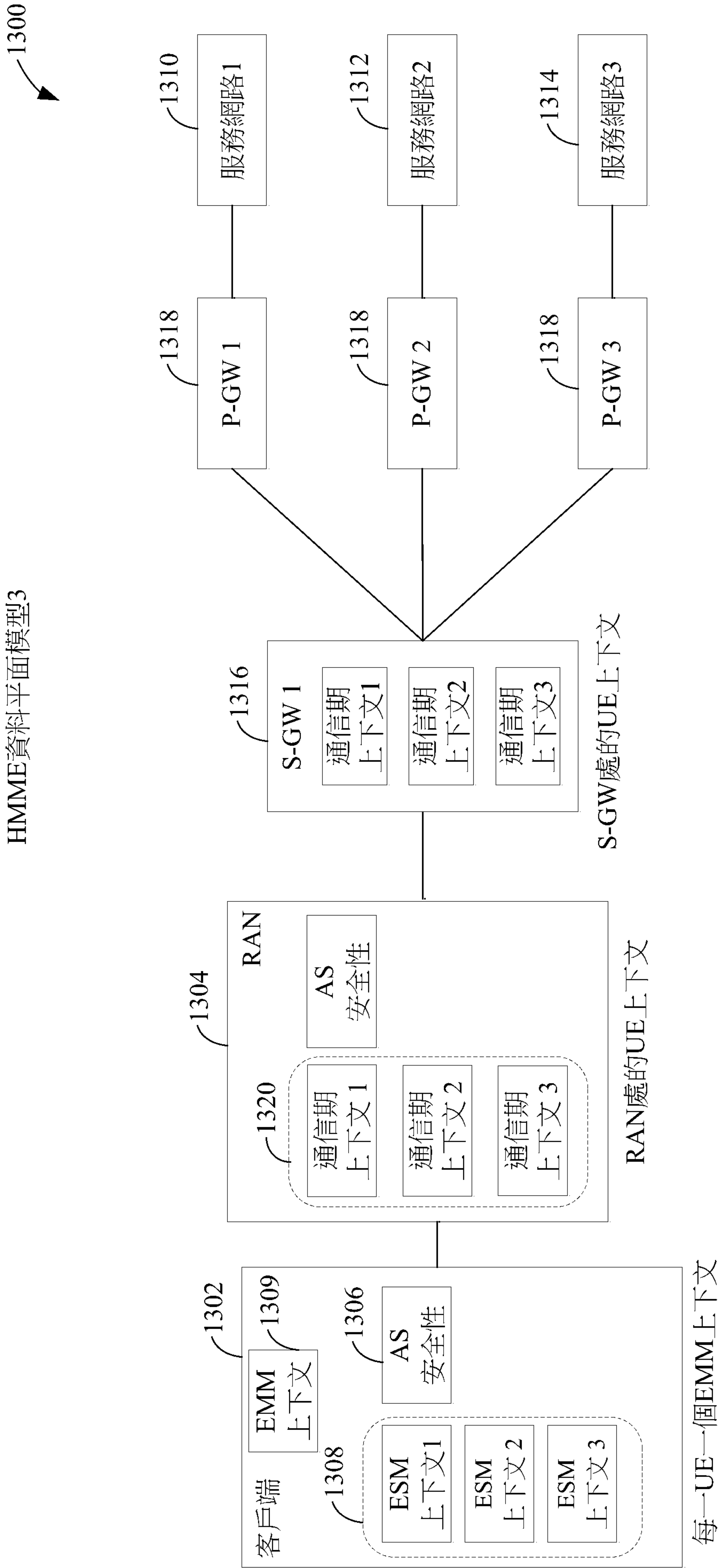


圖17

使用者平面安全性終止於P-GW處

1400

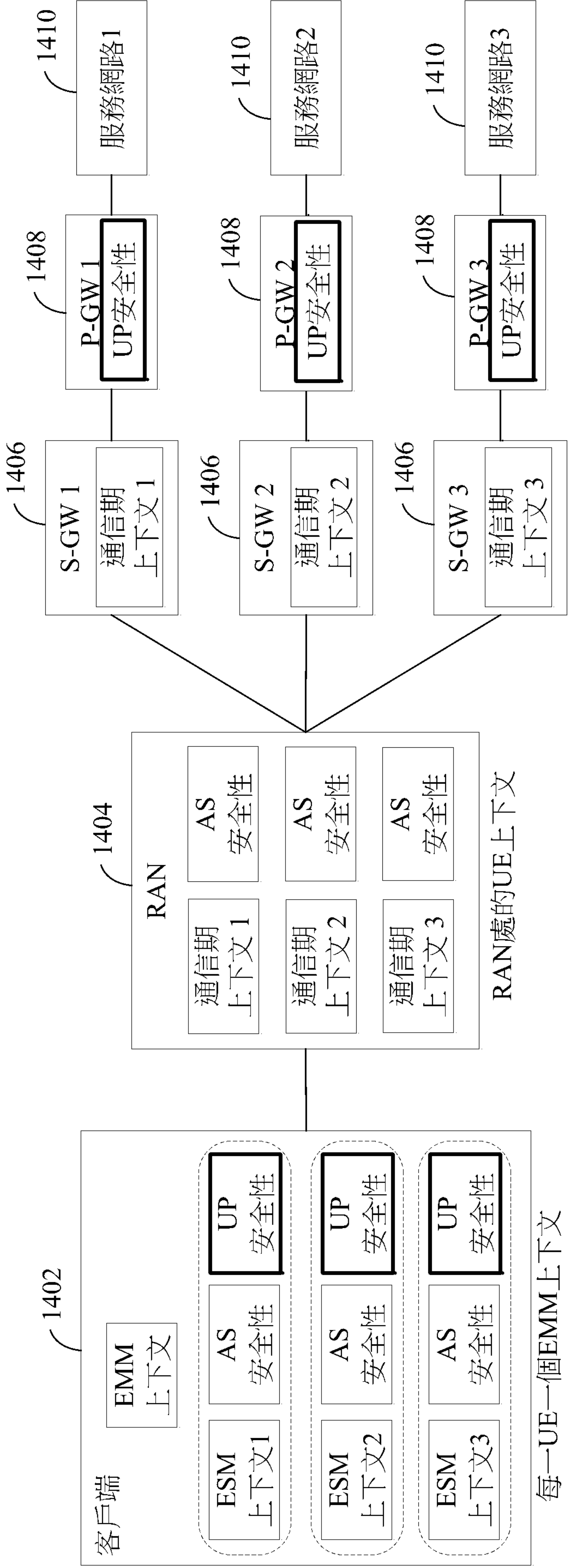


圖18

1500

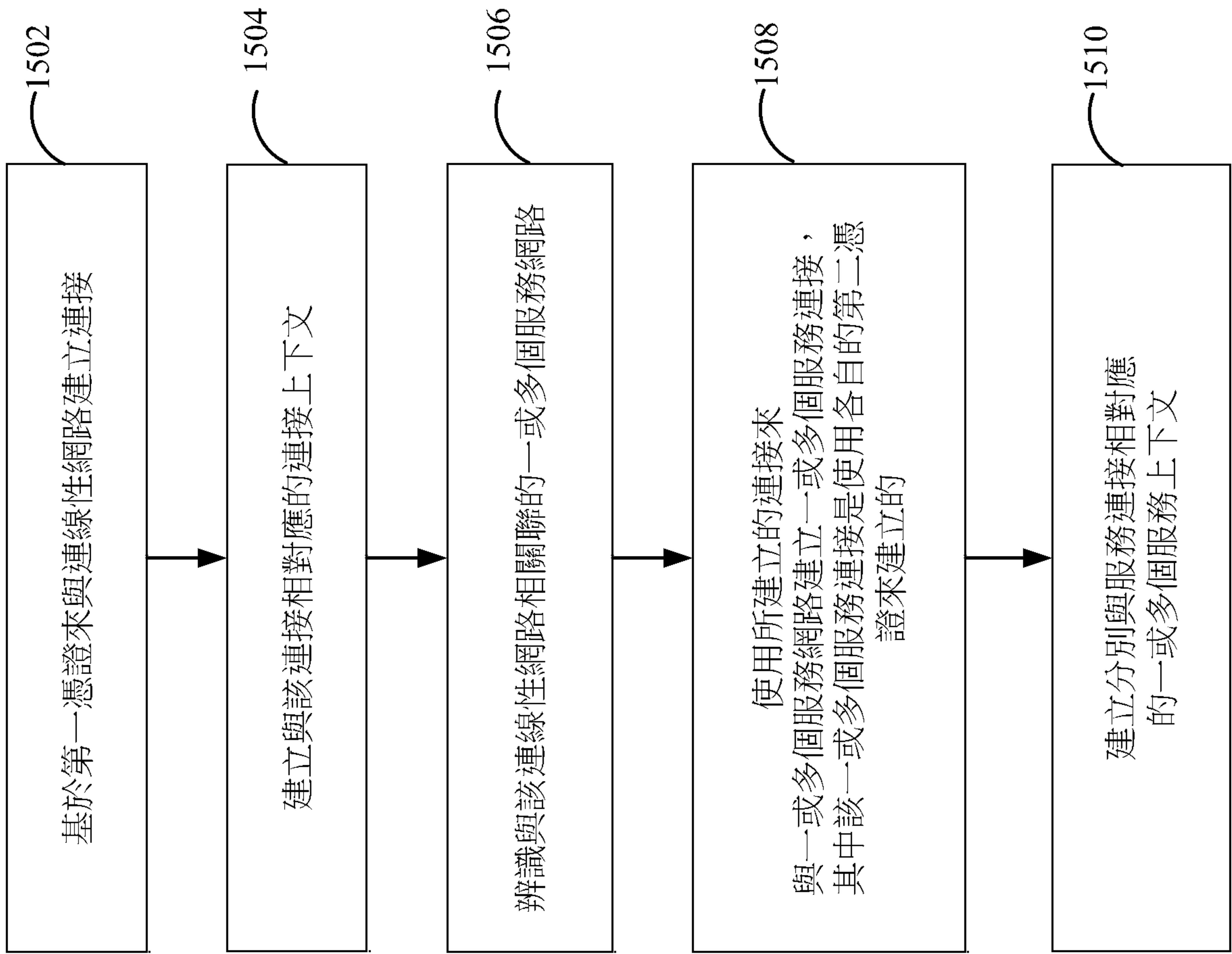


圖19

1500

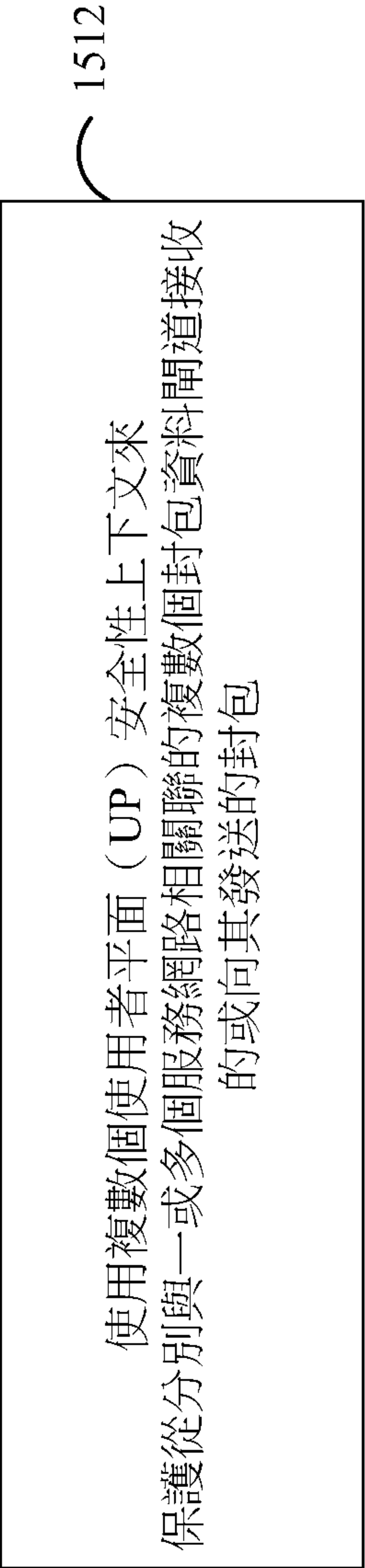


圖20

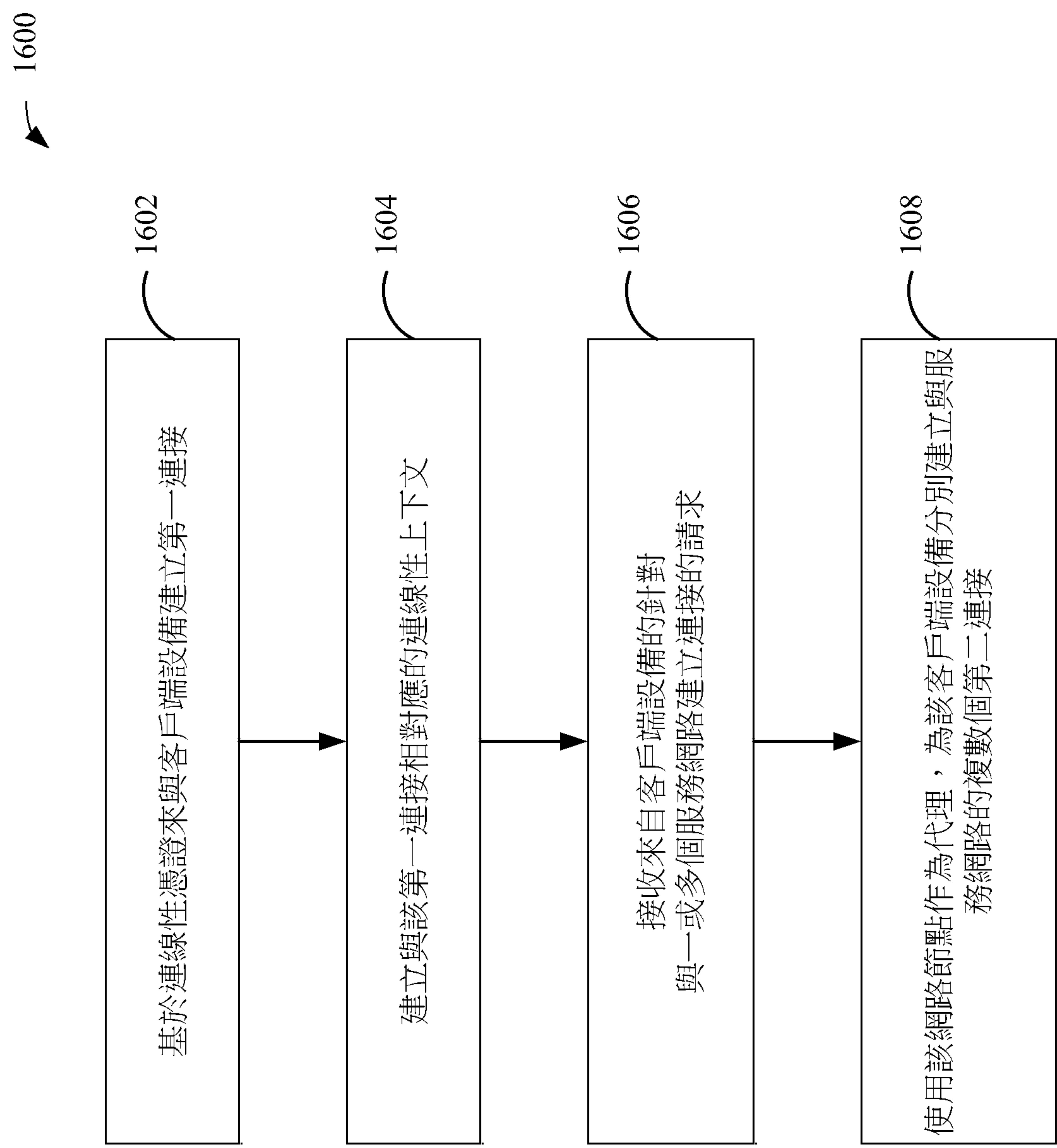


圖21

1600

1610

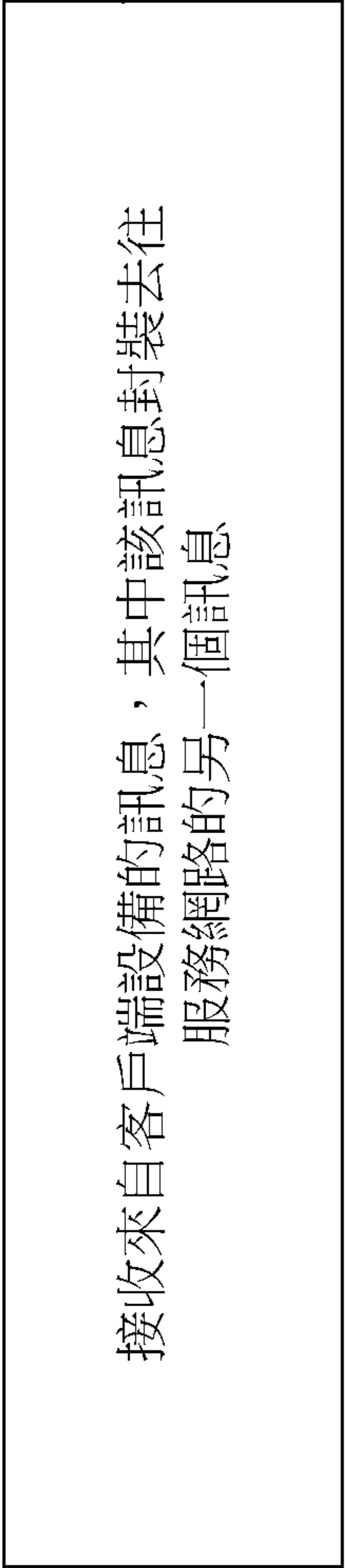


圖22

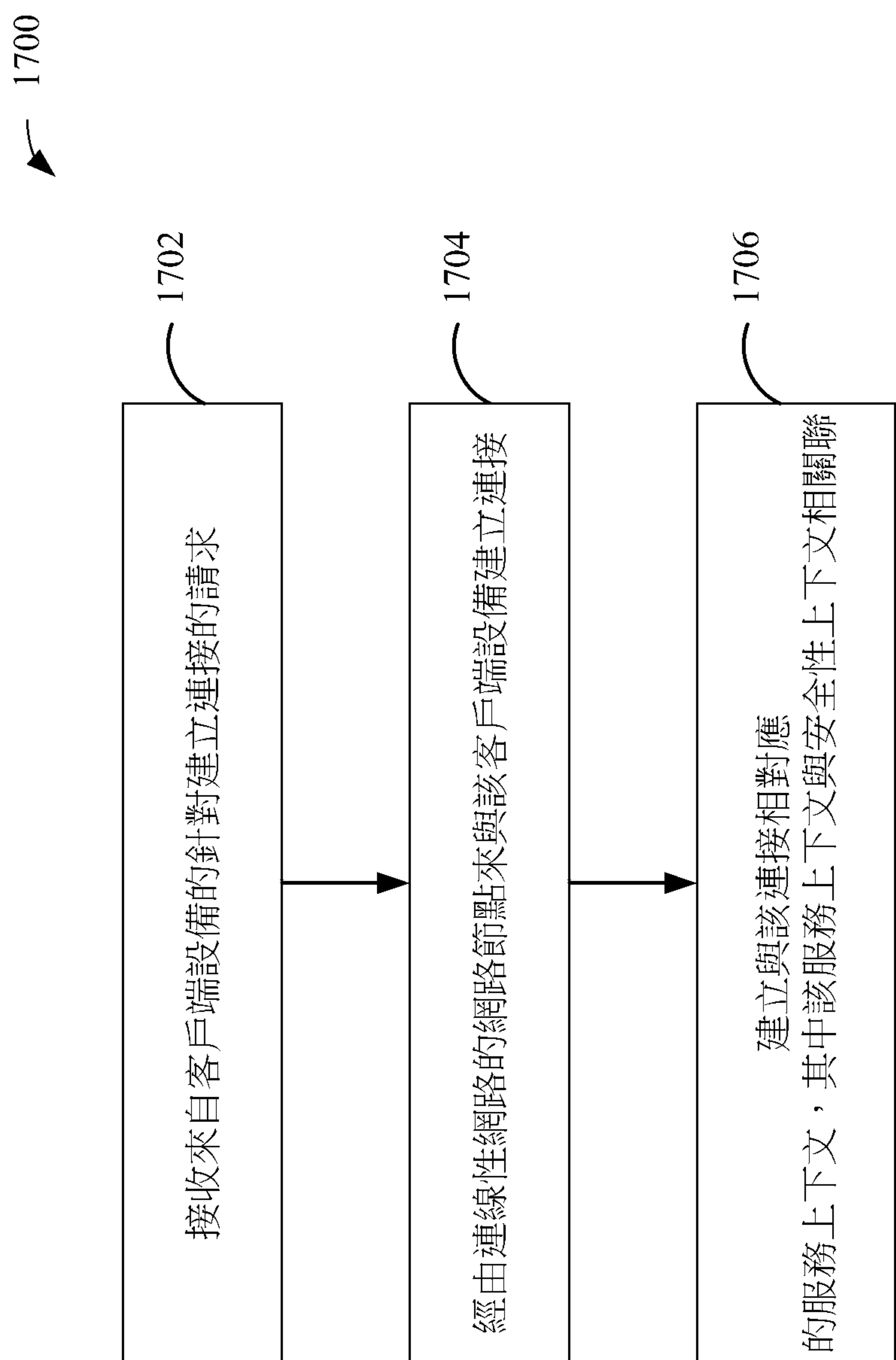


圖23