I492654

(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 I492654 B**

(45)公告日： 中華民國 104 (2015) 年 07 月 11 日

(21)申請案號：100102538 (22)申請日： 中華民國 100 (2011) 年 01 月 24 日

(51)Int. Cl.： *H04W88/04 (2009.01)* *H04W12/06 (2009.01)*

(30)優先權：2010/01/22 美國 61/297,649

2011/01/21 美國 13/011,678

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

美國

(72)發明人：伊史考特愛德利恩 ESCOTT, ADRIAN (GB)；帕拉尼古德艾納德 PALANIGOUNDER, ANAND (IN)；烏魯彼納爾費堤 ULUPINAR, FATIH (US)；羅森伯格布萊恩M ROSENBERG, BRIAN M. (US)

(74)代理人：李世章

(56)參考文獻：

CN 101500229A US 2009/0074189A1

WO 2009/154352A2

審查人員：廖家興

申請專利範圍項數：44 項 圖式數：8 共 53 頁

(54)名稱

用於保障無線中繼節點安全的方法和裝置

METHOD AND APPARATUS FOR SECURING WIRELESS RELAY NODES

(57)摘要

為了減輕通訊網路中中繼節點的插入所引起的安全性風險，設備認證和用戶認證兩者皆在該中繼節點上執行。可將設備認證和用戶認證結合在一起，以使得僅當設備認證和用戶認證兩者皆成功時中繼節點才被容許存取以在網路內進行操作。另外，作為用戶認證過程的一部分，通訊網路(或認證節點)可進一步驗證(作為用戶認證的部分被接收的)用戶識別符與(在相應的設備認證中由設備識別符所識別的)相應的設備類型相關聯。

In order to mitigate the security risk posed by the insertion of a relay node within a communication network, both device authentication and subscriber authentication are performed on the relay node. Device and subscriber authentication may be bound together so that a relay node is granted access to operate within the network only if both device and subscriber authentication are successful. Additionally, a communication network (or authentication node) may further verify that a subscriber identifier (received as part of subscriber authentication) is associated with the corresponding device type (identified by the device identifier in the corresponding device authentication) as part of the subscriber authentication process.

602・・・方塊
604・・・方塊
606・・・方塊
608・・・方塊
610・・・方塊
612・・・方塊

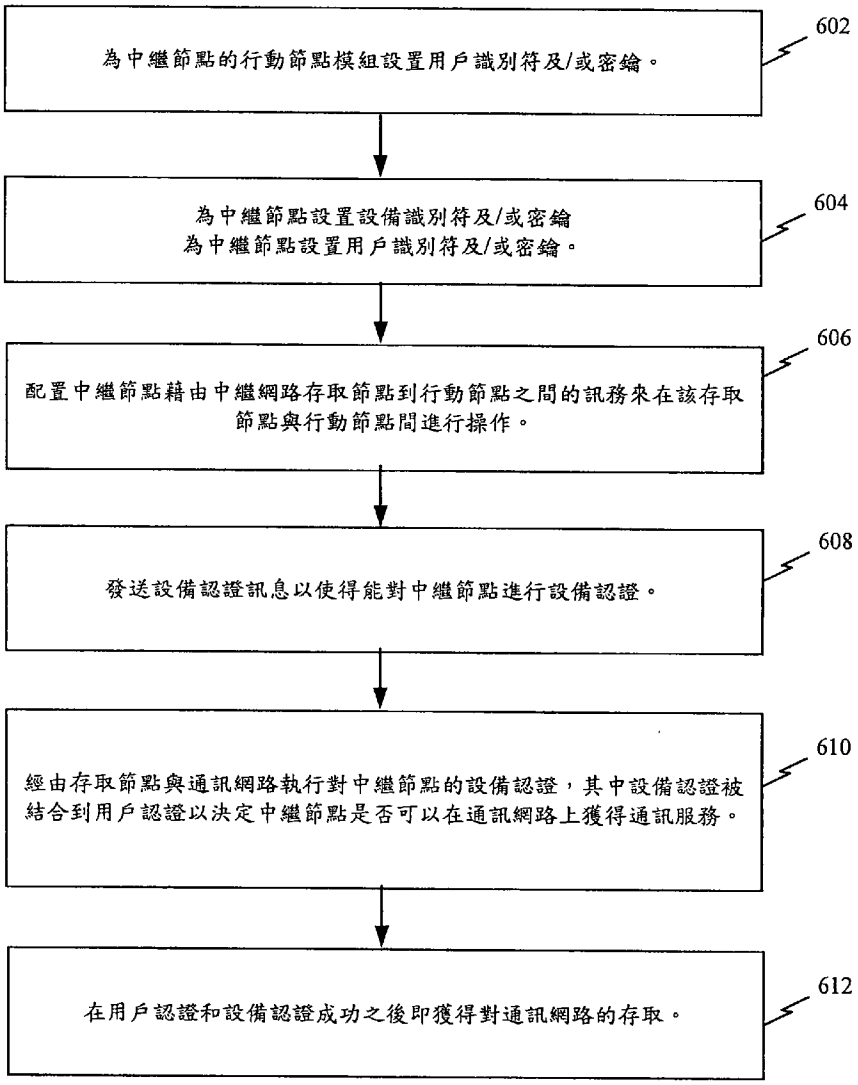


圖6

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：100102538

※ 申請日期：100 年 1 月 24 日 ※IPC 分類：H04W 88/04 (2009.01)
H04W 12/06 (2009.01)

一、發明名稱：（中文/英文）

用於保障無線中繼節點安全的方法和裝置/METHOD AND APPARATUS FOR SECURING WIRELESS RELAY NODES

二、中文發明摘要：

為了減輕通訊網路中中繼節點的插入所引起的安全性風險，設備認證和用戶認證兩者皆在該中繼節點上執行。可將設備認證和用戶認證結合在一起，以使得僅當設備認證和用戶認證兩者皆成功時中繼節點才被容許存取以在網路內進行操作。另外，作為用戶認證過程的一部分，通訊網路（或認證節點）可進一步驗證（作為用戶認證的部分被接收的）用戶識別符與（在相應的設備認證中由設備識別符所識別的）相應的設備類型相關聯。

三、英文發明摘要：

In order to mitigate the security risk posed by the insertion of a relay node within a communication network, both device authentication and subscriber authentication are performed on the relay node. Device and subscriber authentication may be bound together so that a relay node is granted access to operate within the network only if both device and subscriber authentication are successful. Additionally, a communication network (or authentication node) may further verify that a subscriber identifier (received as part of

subscriber authentication) is associated with the corresponding device type (identified by the device identifier in the corresponding device authentication) as part of the subscriber authentication process.

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:

602 方塊

604 方塊

606 方塊

608 方塊

610 方塊

612 方塊

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

根據專利法的優先權主張

本專利申請案主張於 2010 年 1 月 22 日提出申請且被轉讓給本案受讓人並因而被明確以引用之方式併入本文的標題名稱為「Method and Apparatus for Securing Wireless Relays（用於保障無線中繼安全的方法和裝置）」的美國臨時申請案第 61/297649 號的優先權。

【發明所屬之技術領域】

一或多個特徵係關於通訊設備的安全性，且更特定言之係關於用於使使用者裝備無線地介面連接到通訊網路的中繼節點的安全性。

【先前技術】

第三代合作夥伴計畫 3GPP 是已加入此計畫的電信協會群組間的合作，其目的是定義基於進化行動通訊全球系統（GSM）規範並且涵蓋無線電、核心網路和服務架構的全球適用的第三代（3G）行動電話系統規範（例如，在國際電信聯盟（ITU）的國際行動電信-2000 計畫的範疇內）。在 3GPP 內的若干其他標準當中，長期進化（LTE）是行動網路技術領域內的標準。

在 LTE 順應性網路的進化中，中繼節點正在被部署以幫助延伸對使用者裝備的網路覆蓋並增大細胞服務區邊緣頻寬。不同於諸如進化節點 B（eNB）、行動性管理實體（MME）等之類在服務供應商控制的實體位置的控制下操

作的其他網路設備，中繼節點趨向於更靠近使用者裝備地放置在實體上更易存取或更易損的位置並且更獨立地操作。因此，中繼節點易於受到不存在於諸如 eNB 或 MME 之類的其他網路設備中的某些新的安全性威脅和攻擊（例如，中間人攻擊、中繼節點冒名頂替攻擊等）。

【發明內容】

提供了一種在中繼節點中操作的方法。中繼節點可配置為藉由在第一存取節點與第一行動節點之間中繼訊務來在第一存取節點與第一行動節點之間操作。中繼節點的第一通訊介面可調適成與第一存取節點通訊，此中繼節點對第一存取節點表現為第二行動節點。中繼節點的第二通訊介面可調適成與第一行動節點通訊，此中繼節點對第一行動節點表現為第二存取節點。中繼節點可發送設備認證訊息以使得能對此中繼節點進行設備認證。類似地，中繼節點可發送用戶認證訊息以使得能對此中繼節點進行用戶認證，其中設備認證被結合到用戶認證以決定此中繼節點是否可以在通訊網路上獲得通訊服務。在用戶認證和設備認證成功之後，中繼節點即可獲得對通訊網路的存取。例如，在用戶認證和設備認證成功之後，中繼節點即可接收到容許存取通訊網路的服務容許訊息。或者，在用戶認證或設備認證不成功之後，中繼節點即可接收到拒絕存取通訊網路的服務拒絕訊息。設備認證訊息和用戶認證訊息可作為單個認證訊息被同時發送。第一通訊介面可實施與第

二通訊介面不同的空中傳輸（over-the-air）通訊協定。可使用設備識別符或設備密鑰中的至少一者來執行設備認證，此設備識別符或設備密鑰對於中繼節點是唯一性的並儲存於該中繼節點內安全的、不可移除的儲存設備中。設備識別符可以是用於中繼節點、中繼節點內的存取節點模組，或中繼節點內的行動節點模組的國際行動裝備識別碼（IMEI）中的至少一者。第一通訊介面可以是調適成作為長期進化順應性網路的增強型節點B來操作的行動存取模組的部分。第一通訊介面可以是中繼節點的行動節點模組的部分，而第二通訊介面是中繼節點的存取節點模組的部分。用戶認證可隨後較設備認證更頻繁地重複。用戶認證中使用的用戶識別符或密鑰可與設備類型預先關聯，並且僅當設備認證識別出相同的設備類型時用戶認證才成功。

另外，中繼節點可配置為將第一通訊介面上接收的第一封包類型的訊務轉譯為第二封包類型以供在第二通訊介面上傳輸。類似地，中繼節點可配置為將第二通訊介面上接收的第二封包類型的訊務轉譯為第一封包類型以供在第一通訊介面上傳輸。亦即，中繼節點可配置為將第一通訊介面與第二通訊介面之間的資料訊務傳輸從第一信號類型轉譯到第二信號類型。

亦提供了一種在網路認證實體中操作的方法。可由該認證實體接收設備認證訊息，此設備認證訊息由在第一行動節點與第一存取節點間操作的中繼節點啟始。隨後該認證實體可基於與中繼節點、中繼節點的存取節點模組，或中

繼節點的行動節點模組相關聯的一或多個設備識別符或密鑰來執行設備認證。用戶認證訊息亦可在認證實體處被接收，該用戶認證訊息由中繼節點啟始。隨後認證實體可基於與中繼節點相關聯的一或多個用戶識別符或密鑰來執行用戶認證。在用戶認證和設備認證成功之後，則即可發送容許中繼節點存取通訊網路的訊息。或者，在用戶認證或設備認證不成功之後，則可發送拒絕中繼節點存取通訊網路的訊息。用戶認證中使用的用戶識別符或密鑰可與設備類型預先關聯，並且僅當設備認證識別出相同的設備類型時用戶認證才成功。設備認證訊息和用戶認證訊息可作為單個認證訊息被同時接收。

認證實體可向中繼節點發送第一訊息以啟動設備認證；及/或可向中繼節點發送第二訊息以啟動用戶認證。設備認證可由設備認證節點執行，而用戶認證由用戶認證節點執行。

【實施方式】

在以下描述中，提供了特定細節以提供對所描述的實施例的透徹理解。但是，本領域一般技藝人士將可理解，沒有該等特定細節亦可實踐該等實施例。例如，電路可能以方塊圖形式圖示，以免使該等實施例混淆於不必要的細節中。在其他實例中，熟知的電路、結構和技術可能被詳細圖示以免混淆該等實施例。

用語「示例性」在本文中用於意謂「用作示例、實例或

說明」。本文中描述為「示例性」的任何實施或實施例不必被解釋為較佳於或勝過其他實施例。同樣，術語「實施例」並不要求所有實施例皆包括所論述的特徵、優點或操作模式。本文中使用的術語「中繼節點」和「使用者裝備」意謂被寬泛解讀。例如，術語「中繼節點」可代表促進（一或多個使用者裝備）到通訊網路或資料網路的無線連通性的設備。另外，術語「使用者裝備」及/或「行動節點」及/或「客戶終端」可包括行動電話、傳呼機、無線數據機、個人數位助理、個人資訊管理器（PIMs）、掌上型電腦、膝上型電腦、數位平板電腦及/或至少部分地經由無線網路或蜂巢網路通訊的其他行動通訊/計算設備。術語「存取節點」可代表耦合到通訊網路並提供一或多個行動節點到該通訊網路之間的無線連通性的設備

概述

為了減輕通訊網路內插入中繼節點所引起的安全性風險，設備認證和用戶認證兩者皆在該中繼節點上執行。可將設備認證和用戶認證結合在一起以使得僅當設備認證和用戶認證兩者皆成功時中繼節點才被容許存取以在網路內進行操作。另外，作為用戶認證過程的一部分，通訊網路（或認證節點）可進一步驗證（作為用戶認證的部分被接收的）用戶識別符與（在相應的設備認證中由設備識別符所識別的）相應的設備類型相關聯。

具有中繼節點的示例性通訊網路

圖 1 是具有中繼節點的示例性通訊網路的方塊圖。通訊

網路 100 可包括 IP 通訊網路 102（例如長期進化（LTE）相容網路）、使用者-UE 服務閘道（SGW）/PDN 閘道（PGW）126、施主 eNB 128（亦稱作存取節點）、中繼節點 120 和使用者裝備（使用者-UE）104（亦稱作行動節點）。中繼節點 120 經由施主 eNB 128 和使用者-UE 服務閘道（SGW）/PDN 閘道（PGW）126 耦合到通訊網路 102。對於通訊網路 102 和施主 eNB 128，中繼節點 120 可表現為使用者裝備（例如，UE）。對於使用者裝備（使用者-UE）104，中繼節點 120 可表現為增強型節點 B（eNB）。為達到該目的，中繼節點 120 可包括（對 UE 104 表現為網路閘道的）eNB 模組 122 和（對網路 102 表現為 UE 的）的 UE 模組 124。

從通訊網路 102 的角度來看，中繼節點 120 表現為使用者裝備。去往/來自中繼節點 120 和通訊網路 102 的通訊是經由 UE 模組 124（例如，使用進化通用地面存取（E-UTRA）Un 信號協定/介面）來執行的。

類似地，從使用者-UE 104 的角度來看，中繼節點 120 表現為網路 eNB。去往/來自中繼節點 120 和使用者-UE 104 的通訊是經由 eNB 模組 122（例如，使用進化通用地面存取（E-UTRA）Uu 信號協定/介面）來執行的。儘管 eNB 通常是由有線連接（例如，光纖連接等）耦合到通訊網路 102，但是中繼節點可使用空中傳輸（over-the-air）訊號傳遞（例如，LTE 順應性協定）來與 eNB 進行通訊。

在一個實例中，施主 eNB 128 可包括 eNB 116、中繼-UE SGW/PGW 114 及/或中繼閘道 112 的功能性。中繼閘道 112

和使用者-UE SGW/PGW 126之間的通訊可使用S1-U(UE)信號協定/介面。類似地，eNB 116與中繼-UE SGW/PGW 114之間的通訊可使用S1-U（中繼）信號協定/介面。

E-UTRA Uu和Un分別代表使用者-UE 104與中繼節點120之間以及中繼節點120與施主-eNB 128之間的典型訊號傳遞協定/介面。E-UTRA Uu和Un介面可以是用於經由無線電提供去往/來自使用者-UE 104的封包資料服務的LTE網路介面。

3GGP技術規範（TS）36.41x系列技術規範亦定義了用於進化通用地面無線電存取網路（E-UTRAN）的進化節點B(eNB)元件到系統架構進化(SAE)/進化封包核心(EPC)系統的核心網路的互連的S1介面。因此，eNB 116與中繼-UE SGW/PGW 114之間的通訊可使用S1訊號傳遞協定/介面。

在一個實例中，服務閘道（亦即，中繼-UE SGW 114及/或使用者-UE SGW 126）路由並轉發使用者資料封包，同時亦充當eNB間交遞期間針對使用者面的行動性錨點並且充當針對LTE與其他3GPP技術間的行動性錨點(例如，端接S4介面並中繼2G/3G系統和PGW間的訊務)。類似地，PDN閘道（PGW)(例如，中繼-UE PGW 114和使用者-UE PGW 126）可藉由作為UE的訊務出口點和入口點來提供從UE到外部封包資料網路（PDN）的連通性。UE可同時與多於一個PGW具有連通性以存取多個PDN。PGW可執行策略強制、針對每個使用者的封包過濾、收費支

援、合法攔截以及封包篩選。PGW 的另一個角色是充當 3GPP 與諸如 WiMAX 和 3GPP2（CDMA 1X 和 EvDO）之類的非 3GPP 技術間的行動性錨點。

在圖 1 的實例中，通訊網路 102 可調適成辨識使用者-UE 104 是經由施主 eNB 128 耦合的。因此，使用者-UE 行動性管理實體（MME）108 告訴使用者-UE SGW/PGW 126 經由施主 eNB 128 的中繼 GW 112 來轉發使用者-UE 104 的通訊。由於使用者-UE 104 實際上是經由中繼節點 120 連接的，因此中繼-UE 行動性管理實體（MME）118 將中繼-UE SGW/PGW 114 配置成將使用者-UE 104 的通訊路由到中繼節點 120。注意到，正是由於中繼節點 120 表現為另一個 UE(亦即，UE 模組 124)，因此不需要修改施主 eNB 116 協定及/或操作。其允許重用 eNB 和中繼節點處的現有協定/介面。注意到，為說明目的，圖 1 中圖示兩個分開的 MME（亦即，使用者-UE MME 108 和中繼-UE MME 118）。但是，在一些實施例中，由使用者-UE MME 108 和中繼-UE MME 118 執行的功能可被組合到單個 MME 設備中。

許多通訊系統依賴於在容許網路存取前進行用戶/使用者認證。此舉可藉由使用耦合到 UE 或 UE 模組並包含一或多個用於認證用戶/使用者的密鑰（例如，以實施認證和密鑰協定（AKA））的可移除用戶模組或智慧卡（例如，在 LTE 順應性網路中亦被稱為通用積體電路卡（UICC））來做到。在一個實例中，中繼節點 120 中的 UE 模組 124 可包括至少一個此種可移除智慧卡。但是，因為此種用戶

/使用者認證程序被設計為允許使用者/用戶改變/升級 UE（亦即，智慧卡可被移到不同的 UE），所以此可移除智慧卡並不能用於認證 UE 模組 124 或中繼節點 120。

儘管在使用者-UE 104 與施主 eNB 128 之間引入中繼節點 120 促進了網路覆蓋區域的延伸，但是其亦提供了可被利用以獲得對資料傳輸的未經授權的存取的攻擊點。一些此種攻擊包括冒名頂替攻擊和中間人攻擊。

可實施與中繼節點 120 有關的各種安全性特徵以使得經過中繼節點 120 的傳輸如同經過典型的 eNB 的傳輸一樣安全。亦即，不應由於中繼節點插入到通訊系統中而降低或危及通訊系統/網路的安全性。

對通訊網路中的中繼節點的示例性威脅

威脅 1：冒名頂替中繼節點以對附連到中繼節點的使用者-UE 進行攻擊

圖 2 圖示冒名頂替中繼節點以對附連到中繼節點的使用者-UE 進行攻擊的情形。在冒名頂替攻擊中，攻擊者可從可靠中繼節點 120 移除通用積體電路卡（UICC）223 並將其插入不良中繼節點 220。UICC 223 用於向歸屬用戶伺服器（HSS）219 認證服務訂閱。但是，並沒有中繼節點作為設備的認證，僅有對插入到此中繼節點中的 UICC 中的訂閱的認證。因此，通訊網路不能偵測出不良中繼節點 220 並且由此與使用者-UE 104 有關的密鑰被傳遞給不良中繼節點 220。此舉便允許使用者-UE 104 附連到不良中繼節點 220 並且由此危及去往/來自使用者-UE 104 的資料傳輸的

安全性。

威脅 2：Un 介面處的中間人中繼節點攻擊

圖 3 圖示中間人(MitM)中繼節點攻擊。在此種情形中，可靠中繼節點 120 中的真正 UICC 可能已被替換為偽造 UICC 324。此真正 UICC 323 隨後被插入 MitM 中繼節點 320 中。在此種攻擊中，MitM 中繼節點 320 被插在可靠中繼節點 120 與施主 eNB 128 之間。因為攻擊者知道偽造 UICC 324 的根密鑰，所以 MitM 中繼節點 320 可以攔截並解碼去往/來自可靠中繼節點 120 的訊息。MitM 中繼節點 320 可以在可靠中繼節點 120 或施主 eNB 128 任一者皆不知道其的存在的狀態下透通地傳送、接收、查看及/或修改可靠中繼節點 120 與施主 eNB 128 之間的訊務。因此，可能危及來自/去往連接到真正中繼節點 324 的使用者-UE 104 的任何資料傳輸的安全性。注意到，即使與使用者有關的密鑰受到服務於使用者-UE 104 和中繼節點 120 的 MME 108 和 MME 118 之間的安全協定(諸如 IPsec)保護，MitM 中繼節點 320 亦可以查看、修改及/或注入使用者訊務。由該攻擊所說明的安全性要點在於不僅需要對中繼節點 120 進行設備認證，而且所有的來自可靠中繼節點 120 的安全性隧道以真實網路（亦即，施主 eNB 128）為終點，而不是以 MitM 中繼節點 320 為終點。

威脅 3：在中繼節點與施主 eNB 介面之間攔截/注入訊務

再次參見圖 1，中繼節點 120 與施主 eNB 128 之間的介面是基於標準 E-UTRAN 空中介面的。其意謂中繼節點 120

與施主 eNB 128 之間不是所有非無線電資源控制（RRC）訊號傳遞訊務皆受完整性保護。儘管其對於來自使用者-UE 104 的使用者訊務而言是可接受的，但是對於從中繼節點 120 到通訊網路（例如，施主 eNB 128）的訊號傳遞訊務（無論是 S1-AP 還是 X2-AP）是不可接受的。其意謂使用者-UE 104 與施主 eNB 128 之間的介面（亦即，稱為 Un 介面）需要被保護。因此，或者 Un 介面不可以為標準 E-UTRAN UE-eNB 介面，或者需要使用其他某種保護跨在 Un 介面的 S1-AP 和 X2-AP 訊號傳遞的方法。

威脅 4：冒名頂替中繼節點對網路進行攻擊

再次參見圖 2，不良中繼節點 220 可向通訊網路中插入實質上三種類型的訊務。第一，其可以插入去往中繼-UE MME 118 的非存取層（NAS）訊號傳遞。但是，用不良使用者-UE 可以做到相同的攻擊，因此對此種攻擊的考慮對於中繼節點安全性分析並不重要。第二，不良中繼節點 220 可插入 S1-AP 或 X2-AP 訊號傳遞。第三，不良中繼節點 220 亦可插入使用者面訊務以試圖獲得 IP 連通性抑或以另一使用者的名義插入資料。

中繼節點的示例性保障程序

為了減輕或抵消對中繼節點及/或該中繼節點操作所在的核心通訊網路/系統的安全性威脅，可在中繼節點上實施各種安全性措施。因此，本文描述了用於增強中繼節點及/或通訊網路/系統面對各種類型的安全性威脅的安全性的技術、協定及/或方法，以使得中繼節點合乎理想地如同

eNB 一樣安全。

提供此種安全性的一個態樣包括在允許中繼節點在通訊網路上進行通訊前對該中繼節點執行設備認證。例如，可對中繼節點執行設備認證和用戶認證（例如，E-UTRAN認證）兩者。設備和用戶認證的結果可被結合，以使得若任一者失敗，則此中繼節點便不能在通訊網路上進行操作。可以使用密碼技術手段藉由將作為認證過程的一部分而產生的該等密鑰混和起來，抑或使用程序手段，例如由網路（或者諸如 UICC 之類的受網路信任的模組）來驗證設備認證和用戶認證程序兩者皆啟始自相同實體，來執行設備認證與用戶認證的此類結合。注意到，藉由此種結合，威脅 2（亦即，圖 3 中的中間人攻擊）中使用偽造 UICC 的做法使中繼節點不能獲得對通訊網路的存取，因為設備認證將失敗。

在一個實施例中，此種結合可以藉由直接在中繼節點的安全儲存設備或者環境內設置 AKA 密鑰（並實施有關的 AKA「f」函數）來提供，而不是將該等密鑰儲存在可移除 UICC 卡中。藉由將 AKA 密鑰（通常用於用戶認證）放置在中繼節點的安全的、不可移除的儲存設備內，該等 AKA 密鑰亦有效地充當設備密鑰。因此在此種情況下用戶認證亦充當「設備認證」。

在第二個實施例中，可增強 E-UTRAN 安全性程序以使之亦基於儲存在中繼節點中的身份碼來提供設備認證。此舉有效地將 E-UTRAN 安全性程序（例如，用戶認證）與

基於中繼節點的設備識別碼（諸如中繼節點的 UE 模組的 IMEI 或者 eNB 模組的識別碼）的設備認證結合。此種結合減輕了威脅，因為其為通訊網路和中繼節點提供了另一方為真的保證。其解決了威脅 2 和威脅 4 中的一些攻擊。

將設備認證與用戶認證結合的另一個特徵是通訊網路進一步驗證用戶與設備之間的關係的能力。例如，特定的用戶或服務計畫可與中繼節點設備相關聯。因此，作為認證的一部份，通訊網路（例如，認證節點）可確定自身（例如，在用戶認證期間）接收的用戶識別符是否對應於收到的設備識別符所識別的設備。例如，若通訊網路接收到已知與中繼節點設備類型相關聯的用戶識別符，卻接收到相應的用於行動設備（非中繼設備）的設備識別符，則此通訊網路可拒絕向作出請求的設備提供服務。

其他的安全性態樣可進一步在中繼節點與通訊網路間採用安全性協定（諸如 IPsec）以達到保障控制面訊號傳遞安全的目的。例如，3GPP 技術規範 33.401 版本 9.6.0（以引用之方式併入本文），條款 11 定義了使用 IPsec 來保護進化封包系統（EPS）和 E-UTRAN 相容網路的 S1 和 X2 控制面。此安全性措施阻止或防止了以上提到的威脅 1、3 和 4。由使用控制訊號傳遞面上的 IPsec 引起的管理負擔是可忽略的，因為相比於使用者面訊務而言其控制訊號傳遞極少。在另一個實例中，可在 S1-U 介面和 X2-U 介面中實施使用者面上的 IPsec（針對訊務），如在 3GPP 技術規範 33.401 的條款 12 中所描述的。儘管由於在小的使用者

面封包上使用 IPsec 造成的管理負擔，如此做可能並非對所有的部署均適合，但是當在 LTE 上將不攜帶媒體訊務（諸如 RTP）時其可能是合理的部署解決方案。其亦具有不需要在巨集網路上進行協定增強的優勢。對控制面和使用者面兩者均使用 IPsec 在如下意義上解決了威脅 2：儘管可能仍然有 MitM 節點，但是 MitM 中繼節點中可獲得的所有與真 UE 有關的訊務均受到保護。另外，該解決方案亦藉由使服務於此中繼節點的 P-GW 路由其自身的訊務通過服務供應商網路中的安全性閘道減輕了威脅 3 和威脅 4 中的插入訊務攻擊。此舉確保了任何插入訊務皆被丟棄，因其沒有受到 IPsec 的保護。

圖 4 圖示如何可藉由實施設備認證來保障中繼節點安全以對抗攻擊者的實例。此處，中繼節點 404 可無線地在行動節點 402 與存取節點 406 之間轉送訊務。此存取節點 406 可在核心通訊網路 408 與中繼節點 404 之間傳送訊務。注意到，核心通訊網路 408 可為歸屬網路、受訪網路及/或歸屬網路和受訪網路之一或兩者中的元件或節點。

在一個實例中，中繼節點 404 可包括與存取節點 406 通訊的第一通訊介面（例如，行動節點模組或 UE 模組）以及與行動節點 402 通訊的第二通訊介面（例如，存取節點模組或 eNB 模組）。因此，中繼節點 404 可對存取節點 406 表現為行動節點，且其可對行動節點 402 表現為網路存取節點。例如，第一通訊介面可實施與第二通訊介面不同的空中傳輸通訊協定。因此，中繼節點可執行第一通訊介面

與第二通訊介面之間的信號、訊息及/或封包的轉譯。

在能夠提供中繼服務之前，中繼節點 404 可執行與核心通訊網路 408 進行的認證程序。例如，核心通訊網路 408 可包括歸屬網路及/或受訪網路中負責及/或配置為認證用戶及/或設備的實體。例如，在 LTE 相容網路內可能直接或間接涉及認證程序中的該等實體中的一些實體，包括進化節點 B（eNB）、行動性管理實體（MME）及/或歸屬用戶伺服器。

在能夠提供中繼服務之前，中繼節點 404 可參與到與核心通訊網路 408 進行的設備認證程序 410 中。此設備認證程序 410 可尋求與核心通訊網路 408 認證中繼節點 404。此類設備認證程序 410 可使用一或多個（例如儲存在中繼節點的安全儲存設備中的）因中繼節點（或中繼節點的元件）而異的設備識別符及/或密鑰，以與核心通訊網路 408 認證中繼節點 404。例如，該一或多個設備識別符及/或密鑰可被儲存於中繼節點 404 中的不可移除的儲存設備及/或使用者不可存取的儲存設備內。此舉防止攻擊者試圖獲得對中繼節點處的設備識別符及/或密鑰的存取。在一些實例中，中繼節點的唯一性設備識別符可以是行動節點模組的國際行動裝備識別碼（IMEI）及/或存取節點模組的識別碼，並可以與設備密鑰安全結合。在一些實例中，訂閱識別符可以是國際行動用戶識別碼（IMSI）（例如，永久性訂閱識別碼）及/或全球唯一性臨時 UE 識別碼（GUTI）（例如，LTE 中所使用的臨時訂閱識別碼）。

在一些實施例中，中繼節點 404 可單方面地或獨立地向核心通訊網路 408 發送設備認證訊息以啟動設備認證過程 410。在其他實施例中，核心通訊網路 408 可藉由請求中繼節點 404 發送設備認證訊息來啟動設備認證程序。例如，核心通訊網路 408 可向中繼節點 404 發送質詢訊息（challenge message）。隨後中繼節點 404 使用來自該質詢的資訊（例如，資料、值、函數等）以及自身的一或多個設備識別符/密鑰來產生發送至核心通訊網路 408 的設備認證訊息。例如，中繼節點 404 簡單地用自身的設備密鑰對自身的設備識別符（以及亦可能有在質詢訊息中接收到的其他資訊）進行密碼術簽名，並將包括此設備密鑰和經簽名的設備密鑰的認證訊息發送到核心通訊網路 408。隨後核心通訊網路 408 藉由使用該核心通訊網路 408 已知且與中繼節點 404 相關聯的設備密鑰驗證該經簽名的設備識別符來對中繼節點 404 進行認證。可使用其他的密碼術方法及/或演算法，其中用戶密鑰可以是對稱密鑰（例如，機密密鑰）或者非對稱密鑰（例如，公鑰/私鑰對）。

另外，中繼節點 404 亦可參與到用戶認證程序 412 中。用戶認證程序 412 可尋求與核心通訊網路 408 認證中繼節點 404 的使用者/用戶（例如，該中繼節點的行動節點模組或 UE 模組）。此類用戶認證訊息 412 可使用（例如，儲存於該中繼節點的行動節點模組或 UE 模組中的）一或多個因（與中繼節點或行動節點模組相關聯的）用戶而異的識別符及/或密鑰來與核心通訊網路 408 認證其自身。例如，

該一或多個用於用戶認證的識別符及/或密鑰可被儲存於可移除智慧卡中。

在一些實施例中，中繼節點 404 可單方面地或獨立地向核心通訊網路 408 發送用戶認證訊息以啟動用戶認證過程 412。在其他實施例中，核心通訊網路 408 可藉由請求中繼節點 404 發送用戶認證訊息來啟動用戶認證程序 412。例如，核心通訊網路 408 可向中繼節點 404 發送質詢訊息。隨後中繼節點 404 使用來自該質詢的資訊（例如，資料、值、函數等）以及自身的一或多個用戶識別符/密鑰來產生發送至核心通訊網路 408 的用戶認證訊息。例如，中繼節點 404 簡單地用自身的用戶密鑰對自身的用戶識別符（以及亦可能有在質詢訊息中接收到的其他資訊）進行密碼術簽名，並將包括用戶密鑰和經簽名的用戶密鑰的認證訊息發送到核心通訊網路 408。隨後核心通訊網路 408 藉由使用該核心通訊網路 408 已知且與中繼節點 404 相關聯的用戶密鑰驗證經簽名的用戶識別符來對中繼節點 404 進行認證。可使用其他的密碼術方法及/或演算法，其中用戶密鑰可以是對稱密鑰（例如，機密密鑰）或者非對稱密鑰（例如，公鑰/私鑰對）。

在接收到用戶認證訊息和設備認證訊息之後，核心通訊網路 408 的一或多個元件（例如，一或多個認證節點）即可執行對用戶和設備兩者的認證 414。例如，核心通訊網路 408（或者其一或多個元件）可先存取資訊（例如，密鑰及/或識別碼資訊）來驗證中繼節點 404 及/或其用戶資

訊的真實可靠性。隨後核心通訊網路 408 可發送認證容許/拒絕訊息 416 至其他網路元件（例如，網路存取節點或 eNB）及/或中繼節點 404。若認證已成功，則中繼節點 404 可操作以在行動節點 402 與存取節點 406 之間發送訊務傳輸 418a 和訊務傳輸 418b 至核心通訊網路 408。在一些實施例中，中繼節點 404 可執行其第一通訊介面與其第二通訊介面之間的訊務轉譯 419 以在相異的訊務傳輸間進行轉換。若認證失敗，則中繼節點 404 被拒絕存取從而不得向核心通訊網路 408 傳送訊務。照此方式，核心通訊網路 408 將設備認證結合到用戶認證。若該兩個認證中任一認證失敗，則中繼節點被拒絕存取從而不得在存取節點 406 上傳送訊務。

在一些實施例中，設備認證 410 在用戶認證 412 之前執行。藉由首先執行設備認證，核心網路就可確定請求認證的設備的類型特性。其對於通訊網路隨後確定（例如，作為用戶認證程序的部分被接收的）對應的用戶識別符是否正在與正確的設備類型聯用會是有幫助的。例如，若用戶識別符意謂用於中繼節點設備，但是正與用於行動節點的設備識別符聯用，則設備/用戶認證被拒絕。在其他實施例中，可在設備認證之前執行用戶認證。在另一個替代實施例中，設備認證和用戶認證兩者皆可被組合到單個認證程序/訊息中，由此其同時發生。用於中繼節點設備認證的密碼術密鑰可以是對稱密鑰（例如，機密密鑰）或者非對稱密鑰（例如，公鑰/私鑰對）。

用戶認證更新程序420可隨後（例如，每天或每兩天）被重複以進行持續驗證。類似地，設備認證程序422亦可（例如，每周或每月）被重複，但是不如用戶認證420頻繁。

示例性中繼節點及其中的操作

圖5是圖示一種示例性中繼節點的方塊圖。中繼節點500可包括耦合到行動節點模組506、存取節點模組508及/或內部的安全儲存設備504的處理電路502。行動節點模組506可包括第一通訊介面507，該第一通訊介面507包括發射機和接收機，用於經由第一天線510進行去往/來自存取節點的通訊。行動節點模組506可亦包括行動節點(MN)處理電路503，該行動節點處理電路503可控制去往/來自第一通訊介面的資料轉送及行動節點模組506的其他功能/操作等。行動節點模組506可亦包括儲存設備518，在其中其可維護一或多個唯一性地識別行動節點模組506的行動節點設備識別符。另外，行動節點模組506可耦合到可移除UICC卡514或與其通訊，用戶/使用者認證資訊（例如，密鑰和訂閱識別符）可儲存在可移除UICC卡514中。

類似地，存取節點模組508可包括第二通訊介面509，該第二通訊介面509包括發射機和接收機，用於經由第二天線512進行去往/來自行動節點的通訊。存取節點模組508可亦包括存取節點（AN）處理電路505，該存取節點處理電路505可控制去往/來自第二通訊介面的資料轉送及存取節點模組508的其他功能/操作等。存取節點模組

508 可亦包括儲存設備 520，在其中其可維護一或多個唯一性地識別存取節點模組 506 的存取節點設備識別符。

中繼節點 500 可亦包括耦合到行動節點模組 506、存取節點模組 508 及/或儲存設備 504 的處理電路 502。處理電路 502 可調適成在存取節點模組 508 與行動節點模組 506 之間轉送資料，有可能是藉由將儲存設備 504 用作緩衝器或佇列來進行。另外，處理電路 502 可包括在存取節點模組 508 與行動節點模組 506 之間轉譯訊務格式/協定的訊務轉譯電路 520。例如，訊務轉譯電路 520 可在第一通訊介面 507 與第二通訊介面 509 之間將資料訊務傳輸從第一信號類型轉譯到第二信號類型。

注意到，儘管行動節點模組 506、處理電路 502 和存取節點模組 508 在圖 5 中被圖示為分開的元件或電路，但是其功能及/或操作可被組合到單個電路（例如，積體電路）中。

儲存設備 504 可以亦包括一或多個唯一性地識別中繼節點 500、存取節點模組 508 及/或行動節點模組 506 的設備識別符 516。該一或多個設備識別符 516、一或多個行動節點設備識別符 518 及/或一或多個存取節點設備識別符 520 可由中繼節點用在設備認證的執行中。因為該等識別符和與設備識別符相關聯的密鑰被內部地且安全地儲存（亦即，該等密鑰對於攻擊者而言是不可存取的），所以其對於攻擊者不可用。與設備識別符相關聯的密鑰可以是非對稱密鑰或者對稱密鑰。一或多個該等識別符可被用於

對中繼節點 500 的設備認證，而（UICC 卡 514 中的）用戶/使用者資訊可用於用戶/使用者認證。

圖 6 圖示在中繼節點中操作的藉由執行設備認證來減輕攻擊的方法。中繼節點可在網路存取節點與行動節點之間進行操作。中繼節點可包括存取節點模組和行動節點模組。中繼節點的行動節點模組可包括調適成與存取節點通訊的第一通訊介面。行動節點模組使得中繼節點對存取節點表現為行動節點。中繼節點的存取節點模組亦可包括與行動節點通訊的第二通訊介面，此中繼節點對行動節點表現為網路存取節點。

中繼節點及/或行動節點模組可設有用戶識別符及/或密鑰 602。例如，此類用戶識別符及/或密鑰可被儲存於耦合到行動節點模組的可移除卡中。中繼節點、存取節點模組及/或行動節點模組可亦設有一或多個設備識別符及/或關聯的密鑰 604。例如，此類設備識別符/密鑰可被儲存於中繼節點、行動節點模組及/或存取節點模組內的一或多個安全位置。與設備識別符相關聯的密鑰可以是非對稱密鑰或者對稱密鑰。

中繼節點可配置為在網路存取節點與行動節點之間傳送、轉譯、中繼及/或路由訊務 606。例如，中繼節點及/或其中的行動節點模組可包括調適成與存取節點通訊的第一通訊介面，中繼節點對存取節點表現為行動節點。類似地，中繼節點及/或其中的存取節點模組可包括與行動節點通訊的第二通訊介面，中繼節點對行動節點表現為網路

存取節點。

在被允許在網路上通訊之前，中繼節點可發送一或多個訊息用於設備認證及/或用戶認證。例如，中繼節點可發送設備認證訊息以使得能對中繼節點進行設備認證 608。例如，可經由存取節點將設備認證訊息發送到通訊網路中的第一 MME。類似地，中繼節點可發送用戶認證訊息以使得能對中繼節點（或者至少一個其中的行動節點模組）進行用戶認證，其中設備認證被結合到用戶認證以決定中繼節點是否可以在通訊網路上獲得通訊服務 610。

隨後在用戶認證和設備認證成功之後，中繼節點即可獲得對通訊網路的存取 612。例如，在用戶認證和設備認證成功之後，中繼節點即可接收到容許存取通訊網路的服務容許訊息。或者，在用戶認證或設備認證不成功之後，中繼節點則可接收到拒絕存取通訊網路的服務拒絕訊息。在一個實例中，設備認證訊息和用戶認證訊息可作為單個認證訊息被同時發送。

第一通訊介面可實施與第二通訊介面不同的空中傳輸通訊協定。可使用設備識別符或設備密鑰中的至少一者來執行設備認證，該設備識別符或設備密鑰對於中繼節點是唯一性的並儲存於中繼節點內安全的、不可移除的儲存設備中。設備識別符可以是用於中繼節點、中繼節點內的存取節點模組，或中繼節點內的行動節點模組的國際行動裝備識別碼（IMEI）中的至少一者。第一通訊介面可以是調適成作為長期進化順應性網路的增強型節點 B 來操作的行

動存取模組的一部分。第一通訊介面可以是中繼節點的行動節點模組的一部分，而第二通訊介面是中繼節點的存取節點模組的一部分。用戶認證可隨後較設備認證更頻繁地重複。

另外，中繼節點可配置為將第一通訊介面上接收到的第一封包類型的訊務轉譯為第二封包類型以供在第二通訊介面上傳輸。類似地，中繼節點可配置為將第二通訊介面上接收到的第二封包類型的訊務轉譯為第一封包類型以供在第一通訊介面上傳輸。

示例性核心網路認證設備和其中的操作

圖 7 是圖示根據至少一個實施例的認證節點 700 的選擇元件的方塊圖。認證節點可被實施為一或多個執行與認證節點 700 相同功能的設備。認證節點 700 可包括耦合至通訊介面 708 和儲存設備 704 的處理電路 702。

在一個實例中，處理電路 702 可被實施為處理器、控制器、複數個處理器及/或配置為執行包括例如軟體指令及/或韌體指令的可執行指令的其他結構及/或硬體電路之中的一或多者。處理電路 702 的各種實施例可包括通用處理器、數位信號處理器（DSP）、特殊應用積體電路（ASIC）、現場可程式閘陣列（FPGA）或其他可程式邏輯元件、個別閘門或電晶體邏輯、個別的硬體元件，或其設計成執行本文所描述功能的任何組合。通用處理器可以是微處理器，但在替代方案中，處理器可以是任何一般的處理器、控制器、微控制器，或狀態機。處理器亦可以實施為計算元件

的組合，諸如 DSP 與微處理器的組合、數個微處理器、與 DSP 核心結合的一或多個微處理器，或任何其他此類配置。處理電路 702 的該等實例是用於說明目的並且在本案範疇內的其他合適配置亦是可預期的。

處理電路 702 可調適成經由網路通訊介面 708 從通訊網路接收及/或傳送訊息。為此，網路通訊介面 708 可包括發射機和接收機。在至少一個實施例中，處理電路 702 可包括配置為實施由適當的媒體提供的期望程式編寫的電路。例如，處理電路可包括及/或實施用戶認證模組 710 及/或設備認證模組 712。

在接收到由中繼節點啟始的用戶認證訊息之後，用戶認證模組 710 即可獲得與中繼節點相關聯的隨後用於認證該中繼節點的用戶識別符/密鑰。此類用戶認證可涉及驗證用戶認證訊息中的某些資訊確實自有效用戶啟始。例如，該用戶認證可涉及使用用戶密鑰來重新產生及/或驗證用戶認證訊息中的資訊。

在接收到由中繼節點啟始的設備認證訊息之後，設備認證模組 712 即可獲得一或多個與中繼節點相關聯的中繼節點（RN）設備識別符/密鑰 714、存取節點元件識別符 716 及/或行動節點元件識別符/密鑰 718。該一或多個設備識別符/密鑰隨後用於認證中繼節點。例如，該設備認證可涉及使用設備識別符/密鑰來重新產生及/或驗證設備認證訊息中的資訊。

注意到，在其他的實施例中，用戶認證及/或設備認證可

涉及認證節點 700 與中繼節點之間的一系列訊息。

若用戶認證和設備認證兩者均成功，則認證節點 700 可發送容許該中繼節點存取通訊網路的訊息。

圖 8 圖示在認證節點中操作的藉由執行設備認證來減輕對中繼節點的攻擊的方法。中繼節點可在網路存取節點與行動節點之間操作。中繼節點可包括存取節點模組和行動節點模組。認證節點可獲得中繼節點的一或多個行動節點元件的一或多個用戶識別符/密鑰 802。另外，認證節點可亦獲得一或多個行動節點元件、存取節點元件及/或中繼節點的一或多個設備識別符/密鑰 804。

隨後，認證節點可接收由中繼節點啟始的用戶認證訊息 806。認證節點可隨後使用此一或多個用戶識別符/密鑰來執行用戶認證 808。

另外，認證節點可接收由中繼節點啟始的設備認證訊息 810。認證節點可隨後使用此一或多個設備識別符/密鑰來執行設備認證 812。

在用戶認證和設備認證成功之後，認證節點即可發送容許中繼節點存取通訊網路的訊息 814。

在圖 1、2、3、4、5、6、7 及/或 8 中圖示的元件、步驟、特徵及/或功能中的一或多者可被重新佈局及/或組合成單個元件、步驟或功能，或體現在若干元件、步驟或功能中。亦可添加更多的組件、元件、步驟及/或功能而不會脫離本發明。在圖 1、圖 5 及/或圖 5 中圖示的裝置、設備及/或元件可被配置為執行在圖 4、圖 6 及/或圖 8 中描述的方法、

特徵，或步驟中的一或多者。本文中描述的新穎演算法亦可以高效率地實施在軟體中及/或嵌入硬體中。

亦應注意，至少一些實施例可能是作為被圖示為流程表、流程圖、結構圖，或方塊圖的過程來描述的。儘管流程表可能會把諸操作描述為順序過程，但是該等操作中有許多可以並行或同時執行。另外，該等操作的次序可以被重新安排。過程在其操作完成時終止。過程可對應於方法、函數、程序、子常式、副程式等。當過程對應於函數時，其的終止對應於該函數返回調用方函數或主函數。

此外，諸實施例可由硬體、軟體、韌體、中介軟體、微代碼，或其任何組合來實施。當在軟體、韌體、中介軟體或微碼中實施時，執行必要任務的程式碼或代碼區段可被儲存在諸如儲存媒體或其他儲存設備之類的機器可讀取媒體中。處理器可以執行該等必要的任務。代碼區段可表示程序、函數、副程式、程式、常式、子常式、模組、套裝軟體、軟體組件，或是指令、資料結構，或程式敘述的任何組合。一代碼區段可藉由傳遞及/或接收資訊、資料、引數、參數，或記憶體內容來被耦合到另一代碼區段或硬體電路。資訊、引數、參數、資料等可以經由包括記憶體共享、訊息傳遞、符記傳遞、網路傳輸等任何合適的手段被傳遞、轉發，或傳輸。

術語「機器可讀取媒體」、「電腦可讀取媒體」及/或「處理器可讀取媒體」可包括，但不限於攜帶型或固定的儲存設備、光學儲存設備以及能夠儲存、包含或攜帶指令及/

或資料的各種其他非暫時性媒體。因此，本文中描述的各種方法可部分地或全部地由可儲存在「機器可讀取媒體」、「電腦可讀取媒體」及/或「處理器可讀取媒體」中並由一或多個處理器、機器及/或設備執行的指令及/或資料來實施。

結合本文中揭示的實例描述的方法或演算法可直接在硬體中、在由處理器執行的軟體模組中，或在該兩者的組合中，以處理單元、程式編寫指令，或其他指示的形式體現，並且可包含在單個設備中或跨多個設備分佈。軟體模組可常駐在 RAM 記憶體、快閃記憶體、ROM 記憶體、EPROM 記憶體、EEPROM 記憶體、暫存器、硬碟、可移除磁碟、CD-ROM，或本領域中已知的任何其他形式的儲存媒體中。儲存媒體可耦合到處理器以使得該處理器能從該儲存媒體讀取資訊並向該儲存媒體寫入資訊。在替代方案中，儲存媒體可以被整合到處理器。

本領域技藝人士將可進一步理解，結合本文中揭示的實施例描述的各種說明性邏輯區塊、模組、電路和演算法步驟可被實施為電子硬體、電腦軟體，或兩者的組合。為清楚地說明硬體與軟體的該可互換性，各種說明性元件、方塊、模組、電路和步驟在上文是以其功能性的形式作一般化描述的。此類功能性是被實施為硬體還是軟體取決於特定應用和強加於整體系統的設計約束。

本文中所描述的本發明的各種特徵可實施於不同系統中而不會脫離本發明。應注意，以上實施例僅是實例，且

並不應被解釋成限定本發明。該等實施例的描述意欲成為說明性的，而並非意欲限定請求項的範疇。由此，本發明的教示可以容易地應用於其他類型的裝置，並且許多替代、改動和變形對於本領域技藝人士將是明顯的。

【圖式簡單說明】

圖 1 是具有中繼節點的示例性通訊網路的方塊圖。

圖 2 圖示冒名頂替中繼節點對附連到中繼節點的使用者-UE 進行攻擊。

圖 3 圖示中間人（MitM）中繼節點攻擊。

圖 4 圖示如何藉由實施設備認證來保障中繼節點安全以對抗攻擊者的實例。

圖 5 是圖示示例性中繼節點的方塊圖。

圖 6 圖示在中繼節點中操作的藉由執行設備認證來減輕攻擊的方法。

圖 7 是圖示根據至少一個實施例的認證節點的選擇元件的方塊圖。

圖 8 圖示在認證節點中操作的藉由執行設備認證來減輕對中繼節點的攻擊的方法。

【主要元件符號說明】

100　通訊網路

102　IP 通訊網路

104　使用者裝備（使用者-UE）/UE

108　使用者-UE 行動性管理實體（MME）

112 中繼閘道/中繼 GW

114 中繼-UE SGW/PGW

116 eNB

118 中繼-UE MME

120 中繼節點

122 eNB 模組

124 UE 模組

126 使用者-UE SGW/PGW

128 施主 eNB

219 歸屬用戶伺服器（HSS）

220 不良中繼節點

223 通用積體電路卡（UICC）

320 MitM 中繼節點

323 真正 UICC

324 偽造 UICC

402 行動節點

404 中繼節點

406 存取節點

408 核心通訊網路

410 設備認證過程/設備認證程序

412 用戶認證程序/用戶認證訊息/用戶認證過程/用戶認證

414 對用戶和設備兩者的認證

416 認證容許/拒絕訊息

418a 訊務傳輸

418b 訊務傳輸

419 訊務轉譯

420 用戶認證更新程序/用戶認證

422 設備認證程序

500 中繼節點

502 處理電路

503 行動節點（MN）處理電路

504 儲存設備

505 存取節點（AN）處理電路

506 行動節點模組

507 第一通訊介面

508 存取節點模組

509 第二通訊介面

510 第一天線

512 第二天線

516 設備識別符

520 存取節點設備識別符

602 方塊

604 方塊

606 方塊

608 方塊

610 方塊

612 方塊

700 認證節點

702 處理電路

704 儲存設備

708 網路通訊介面

710 用戶認證模組

712 設備認證模組

714 中繼節點（RN）設備識別符/密鑰

716 存取節點元件識別符

718 行動節點元件識別符/密鑰

802 方塊

804 方塊

806 方塊

808 方塊

810 方塊

812 方塊

814 方塊

103年6月27日修正替換頁

七、申請專利範圍：

1. 一種在一中繼節點中操作的方法，包括以下步驟：

配置該中繼節點藉由在一第一存取節點與一第一行動節點間中繼訊務來在該第一存取節點與該第一行動節點間進行操作，該第一存取節點經配備以提供對一通訊網路之存取，其中

該中繼節點的一第一通訊介面被調適成運用一第一信號協定與該第一存取節點通訊，該中繼節點對該第一存取節點表現為一第二行動節點，及

一第二通訊介面被調適成運用一第二信號協定與該第一行動節點通訊，該中繼節點對該第一行動節點表現為一第二存取節點；

從該中繼節點發送一設備認證訊息到該第一存取節點，以使得能對該中繼節點進行設備認證；及

從該中繼節點發送一用戶認證訊息到該第一存取節點，以使得能對該中繼節點進行用戶認證，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在經由該第一存取節點所存取之該通訊網路上獲得通訊服務，以及其中該中繼節點在同時用戶認證成功及設備認證成功的情況下即得到存取許可與該通訊網路通訊。

2. 如請求項1之方法，進一步包括以下步驟：

在從該第一存取節點接收到指示已經獲准用戶認證

和設備認證成功的信號之後，即獲得對該通訊網路的存取。

3. 如請求項1之方法，進一步包括以下步驟：

在用戶認證和設備認證成功之後即從該第一存取節點接收容許存取該通訊網路的一服務容許訊息；及

在用戶認證或設備認證不成功之後即從該第一存取節點接收拒絕存取該通訊網路的一服務拒絕訊息。

4. 如請求項1之方法，其中該設備認證訊息和該用戶認證訊息是作為一單一認證訊息被同時從該中繼節點發送到該第一存取節點的。

5. 如請求項1之方法，其中該第一通訊介面使用空中傳輸信號與該第一存取節點通訊。

6. 如請求項1之方法，其中設備認證是使用一設備識別符或一設備密鑰中的至少一者來執行的，該設備識別符或該設備密鑰對於該中繼節點是唯一性的並儲存於該中繼節點內一安全的、不可移除的儲存設備中。

7. 如請求項6之方法，其中該設備識別符是用於該中繼節點、該中繼節點內的一存取節點模組，或該中繼節點內的一行動節點模組的國際行動裝備識別碼（IMEI）中的至

少一者。

8. 如請求項 1 之方法，其中該第一通訊介面是一行動存取模組的一部分，該行動存取模組被調適成作為一長期進化順應性網路的一增強型節點 B 來操作。

9. 如請求項 1 之方法，其中該第一通訊介面是該中繼節點的一行動節點模組的一部分，並且該第二通訊介面是該中繼節點的一存取節點模組的一部分。

10. 如請求項 1 之方法，其中用戶認證隨後較設備認證更頻繁地重複。

11. 如請求項 1 之方法，進一步包括以下步驟：

配置該中繼節點將該第一通訊介面上接收到的一第一封包類型的訊務轉譯為一第二封包類型以供在該第二通訊介面上傳輸至該第一行動節點；及

配置該中繼節點將該第二通訊介面上接收到的該第二封包類型的訊務轉譯為該第一封包類型以供在該第一通訊介面上傳輸至該第一存取節點。

12. 如請求項 1 之方法，進一步包括以下步驟：

配置該中繼節點在該第一通訊介面與該第二通訊介面之間將資料訊務傳輸從一第一信號類型轉譯為一第二

信號類型，該第一信號類型關聯於該第一信號協定，該第二信號類型關聯於該第二信號協定。

13. 如請求項 1 之方法，其中用戶認證中使用的一用戶識別符或一密鑰中之一或更多者與一設備類型預先關聯，並且當該設備認證識別出相同的設備類型時用戶認證為成功。

14. 如請求項 1 之方法，其中該第一信號協定及該第二信號協定相同。

15. 如請求項 1 之方法，其中該第一信號協定及該第二信號協定為進化通用地面存取（E-UTRA）通訊協定。

16. 如請求項 1 之方法，其中該第一信號協定及該第二信號協定為不同之空中傳輸通訊協定。

17. 如請求項 1 之方法，其中該中繼節點對該第一存取節點表現為一使用者裝備（UE）。

18. 如請求項 1 之方法，其中該中繼節點對該第一行動節點表現為一增強型節點 B（eNB）。

19. 一種中繼節點，包括：

一第一通訊介面，該第一通訊介面被調適成運用一第一信號協定與一第一存取節點通訊，該中繼節點對該第一存取節點表現為一第二行動節點，該第一存取節點經配備以提供對一通訊網路的存取；

一第二通訊介面，該第二通訊介面被調適成運用一第二信號協定與一第一行動節點通訊，該中繼節點對該第一行動節點表現為一第二存取節點；及

一處理電路，該處理電路耦合至該第一通訊介面和該第二通訊介面，該處理電路被調適成：

在該第一存取節點與該第一行動節點間中繼訊務，

從該中繼節點經由該第一通訊介面發送一設備認證訊息至該第一存取節點，以使得能對該中繼節點進行設備認證，及

從該中繼節點經由該第一通訊介面發送一用戶認證訊息至該第一存取節點，以使得能對該中繼節點進行用戶認證，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在經由該第一存取節點所存取之該通訊網路上獲得通訊服務，以及其中該中繼節點在同時用戶認證成功及設備認證成功的情況下即得到存取許可與該通訊網路通訊。

20. 如請求項19之中繼節點，其中該處理電路被進一步調適成：

在從該第一存取節點接收到指示已經獲准用戶認證

和設備認證成功的信號之後，即獲得對該通訊網路的存取。

21. 如請求項 19 之中繼節點，其中該處理電路被進一步調適成：

在用戶認證和設備認證成功之後即從該第一存取節點接收容許存取該通訊網路的一服務容許訊息；及

在用戶認證或設備認證不成功之後即從該第一存取節點接收拒絕存取該通訊網路的一服務拒絕訊息。

22. 如請求項 19 之中繼節點，進一步包括：

一不可移除的安全儲存設備，該不可移除的安全儲存設備經耦合到該處理電路，該不可移除的安全儲存設備儲存一設備識別符或一密鑰中的至少一者，該設備識別符或該密鑰對於該中繼節點是唯一性的並用於設備認證。

23. 如請求項 22 之中繼節點，其中該設備識別符是用於該中繼節點、該中繼節點內的一存取節點模組，或該中繼節點內的一行動節點模組的國際行動裝備識別碼（IMEI）中的至少一者。

24. 如請求項 19 之中繼節點，其中該第一通訊介面使用空中傳輸信號與該第一存取節點通訊。

25. 如請求項19之中繼節點，進一步包括：

一行動節點模組，該行動節點模組包括該第一通訊介面和一不可移除的儲存設備，該不可移除的儲存設備用於儲存用於設備認證的一或更多個行動節點識別符及密鑰。

26. 如請求項19之中繼節點，進一步包括：

一存取節點模組，該存取節點模組包括該第二通訊介面和一不可移除的儲存設備，該不可移除的儲存設備用於儲存用於設備認證的一或更多個存取節點識別符及密鑰。

27. 如請求項19之中繼節點，其中該處理電路被進一步調適成：

在該第一通訊介面與該第二通訊介面之間將資料訊務傳輸從一第一信號類型轉譯為一第二信號類型，該第一信號類型關聯於該第一信號協定，該第二信號類型關聯於該第二信號協定。

28. 一種中繼節點，包括：

用於運用一第一信號協定與一第一存取節點通訊的構件，該中繼節點對該第一存取節點表現為一第二行動節點，該第一存取節點經配備以提供對一通訊網路之存取；

用於運用一第二信號協定與一第一行動節點通訊的構件，該中繼節點對該第一行動節點表現為一第二存取節點；

用於在該第一存取節點與該第一行動節點之間中繼訊務的構件；

用於從該中繼節點發送一設備認證訊息至該第一存取節點以使得能對該中繼節點進行設備認證的構件；及

用於從該中繼節點發送一用戶認證訊息至該第一存取節點以使得能對該中繼節點進行用戶認證的構件，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在經由該第一存取節點所存取之該通訊網路上獲得通訊服務，以及其中該中繼節點在同時用戶認證成功及設備認證成功的情況下即得到存取許可與該通訊網路通訊。

29. 如請求項28之中繼節點，進一步包括：

用於在從該第一存取節點接收到指示已經獲准用戶認證和設備認證成功的信號之後即獲得對該通訊網路的存取的構件。

30. 如請求項28之中繼節點，進一步包括：

用於安全地且不可移除地儲存一設備識別符或一密鑰中的至少一者的構件。

31. 如請求項28之中繼節點，進一步包括：

用於在該第一通訊介面與該第二通訊介面之間將資料訊務傳輸從一第一信號類型轉譯為一第二信號類型的構件，該第一信號類型關聯於該第一信號協定，該第二信

號類型關聯於該第二信號協定。

32. 一種處理器可讀取儲存媒體，該處理器可讀取儲存媒體包括一或更多個在一中繼節點上操作的指令，該中繼節點被調適成在一第一行動節點與一第一存取節點間操作，其中該一或更多個指令在被一處理電路執行時使該處理電路：

運用一第一信號協定經由一第一通訊介面與一第一存取節點通訊，該中繼節點對該第一存取節點表現為一第二行動節點，該第一存取節點經配備以提供對一通訊網路之存取；

運用一第二信號協定經由一第二通訊介面與一第一行動節點通訊，該中繼節點對該第一行動節點表現為一第二存取節點；

在該第一存取節點與該第一行動節點之間中繼訊務；

從該中繼節點經由該第一通訊介面發送一設備認證訊息至該第一存取節點，以使得能對該中繼節點進行設備認證；及

從該中繼節點經由該第一通訊介面發送一用戶認證訊息至該第一存取節點，以使得能對該中繼節點進行用戶認證，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在經由該第一存取節點所存取之該通訊網路上獲得通訊服務，以及其中該中繼節點在同時用戶認證成功及設備認證成功的情況下即得到存取許可與該通訊

網路通訊。

33. 如請求項32之處理器可讀取儲存媒體，該處理器可讀取儲存媒體包括在被一處理電路執行時使該處理電路執行以下操作的一或更多個指令：

在從該第一存取節點接收到指示已經獲准用戶認證和設備認證成功的信號之後，即獲得對該通訊網路的存取。

34. 一種在一網路認證實體中操作的方法，包括以下步驟：

接收由一中繼節點啟始的一設備認證訊息，該中繼節點在一第一行動節點與一第一存取節點間操作，其中該中繼節點經配置以分別運用第一信號協定及第二信號協定在該第一行動節點及該第一存取節點間通訊，以及其中該第一存取節點經配備以提供對一通訊網路之存取；

基於與該中繼節點、該中繼節點的一存取節點模組，或該中繼節點的一行動節點模組相關聯的一或更多個設備識別符或密鑰執行設備認證；

接收由該中繼節點啟始的一用戶認證訊息；

基於與該中繼節點相關聯的一或更多個用戶識別符或密鑰執行該中繼節點的用戶認證；及

在用戶認證和設備認證都成功之後即發送容許該中繼節點存取該通訊網路的一訊息，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在該通訊網路

上獲得通訊服務。

35. 如請求項34之方法，進一步包括以下步驟：

在用戶認證或設備認證中之一或更多者不成功之後，即發送拒絕該中繼節點存取該通訊網路的一訊息至該中繼節點。

36. 如請求項34之方法，進一步包括以下步驟：

發送一第一訊息至該中繼節點以啟動設備認證；及

發送一第二訊息至該中繼節點以啟動用戶認證。

37. 如請求項34之方法，其中用戶認證中使用的一用戶識別符或一密鑰中之一或更多者與一設備類型預先關聯，並且當該設備認證識別出該相同的設備類型時用戶認證為成功。

38. 如請求項34之方法，其中設備認證由一設備認證節點執行而用戶認證由一用戶認證節點執行。

39. 如請求項34之方法，其中該設備認證訊息和該用戶認證訊息作為一單一認證訊息被同時接收。

40. 一種認證實體，包括：

一通訊介面，該通訊介面被調適成在一通訊網路上與

一中繼節點通訊；

一處理電路，該處理電路耦合到該通訊介面，該處理電路被調適成：

接收由該中繼節點啟始的一設備認證訊息，該中繼節點在一第一行動節點與一第一存取節點間操作，其中該中繼節點經配置以分別運用第一信號協定及第二信號協定在該第一行動節點及該第一存取節點間通訊，以及其中該第一存取節點經配備以提供對一通訊網路之存取；

基於與該中繼節點、該中繼節點的一存取節點元件，或該中繼節點的一行動節點元件相關聯的一或更多個設備識別符或密鑰，來執行該中繼節點之設備認證；

接收由該中繼節點啟始的一用戶認證訊息；

基於與該中繼節點相關聯的一或更多個用戶識別符或密鑰執行用戶認證，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在該通訊網路上獲得服務；及

在用戶認證和設備認證都成功之後即發送容許該中繼節點存取該通訊網路的一訊息。

41. 如請求項40之認證實體，其中該處理電路被進一步調適成：

在用戶認證或設備認證中之一或更多者不成功之後即發送拒絕該中繼節點存取該通訊網路的一訊息。

42. 如請求項41之認證實體，進一步包括：

一設備認證節點，該設備認證節點用於執行設備認證；及

一用戶認證節點，該用戶認證節點用於執行用戶認證。

43. 一種認證實體，包括：

用於接收由一中繼節點啟始的一設備認證訊息的構件，該中繼節點在一第一行動節點與一第一存取節點間操作，其中該中繼節點經配置以運用一第一信號協定與該第一行動節點通訊，及運用一第二信號協定與該第一存取節點間通訊；

用於基於與該中繼節點、該中繼節點的一存取節點元件，或該中繼節點的一行動節點元件相關聯的一或更多個設備識別符或密鑰執行設備認證的構件；

用於接收由該中繼節點啟始的一用戶認證訊息的構件；

用於基於與該中繼節點相關聯的一或更多個用戶識別符或密鑰執行用戶認證的構件，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在該通訊網路上獲得服務；及

用於在用戶認證和設備認證都成功之後即發送容許該中繼節點存取該通訊網路的一訊息的構件。

44. 一種處理器可讀取儲存媒體，該處理器可讀取儲存媒體包括一或更多個在一認證實體上操作的指令，該認證實體在一核心通訊網路內操作，該等指令在由一處理電路執行時使該處理電路：

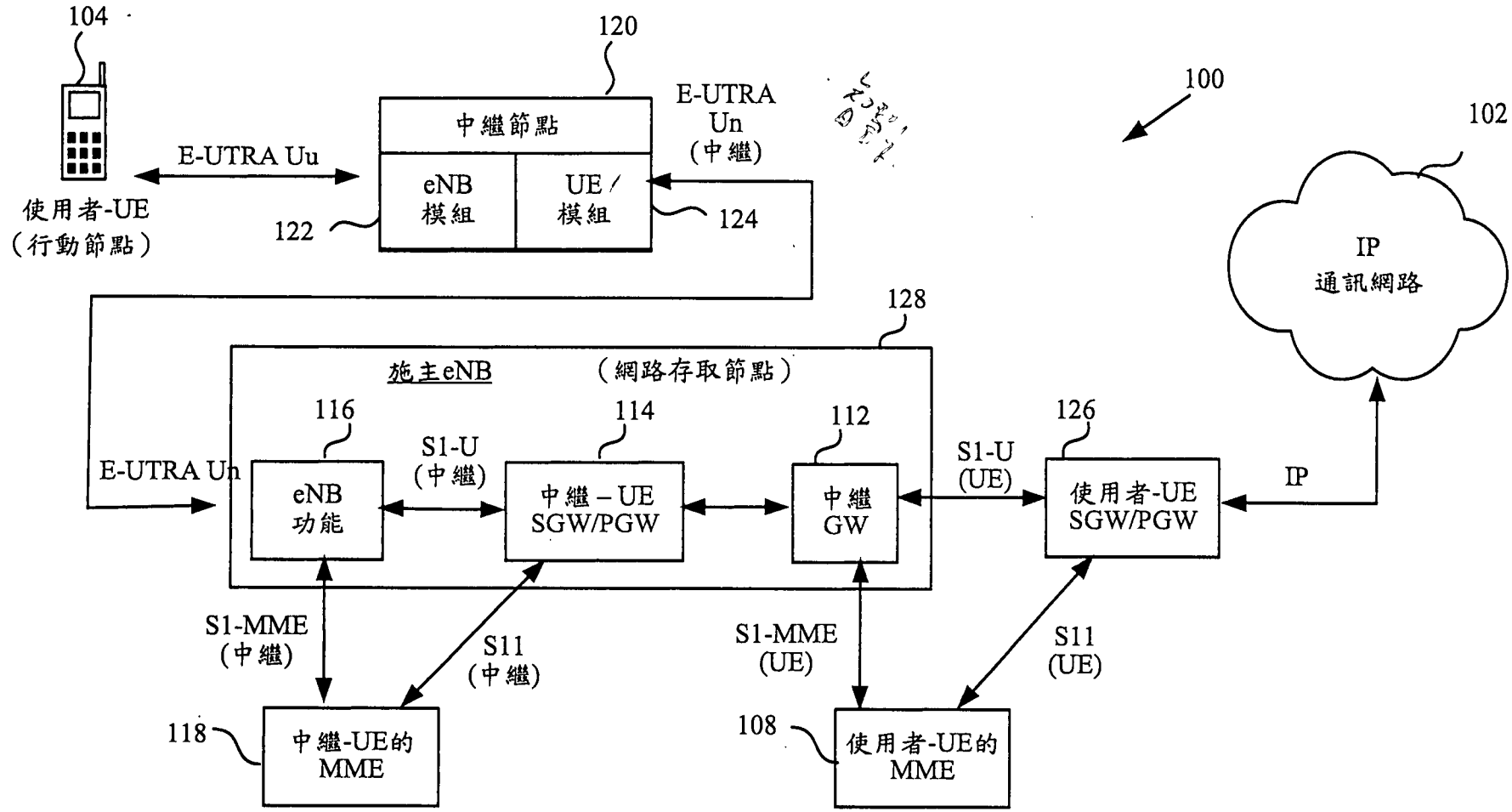
接收由一中繼節點啟始的一設備認證訊息，該中繼節點在一第一行動節點與一第一存取節點間操作，其中該中繼節點經配置以運用一第一信號協定與該第一行動節點通訊，及運用一第二信號協定與該第一存取節點間通訊；

基於與該中繼節點、該中繼節點的一存取節點元件，或該中繼節點的一行動節點元件相關聯的一或更多個設備識別符或密鑰執行設備認證；

接收由該中繼節點啟始的一用戶認證訊息；

基於與該中繼節點相關聯的一或更多個用戶識別符或密鑰執行用戶認證，其中該設備認證被結合到該用戶認證以決定該中繼節點是否可以在該通訊網路上獲得服務；及

在用戶認證和設備認證都成功之後即發送容許該中繼節點存取該通訊網路的一訊息。



具有中繼節點的示例性通訊網路

圖 1

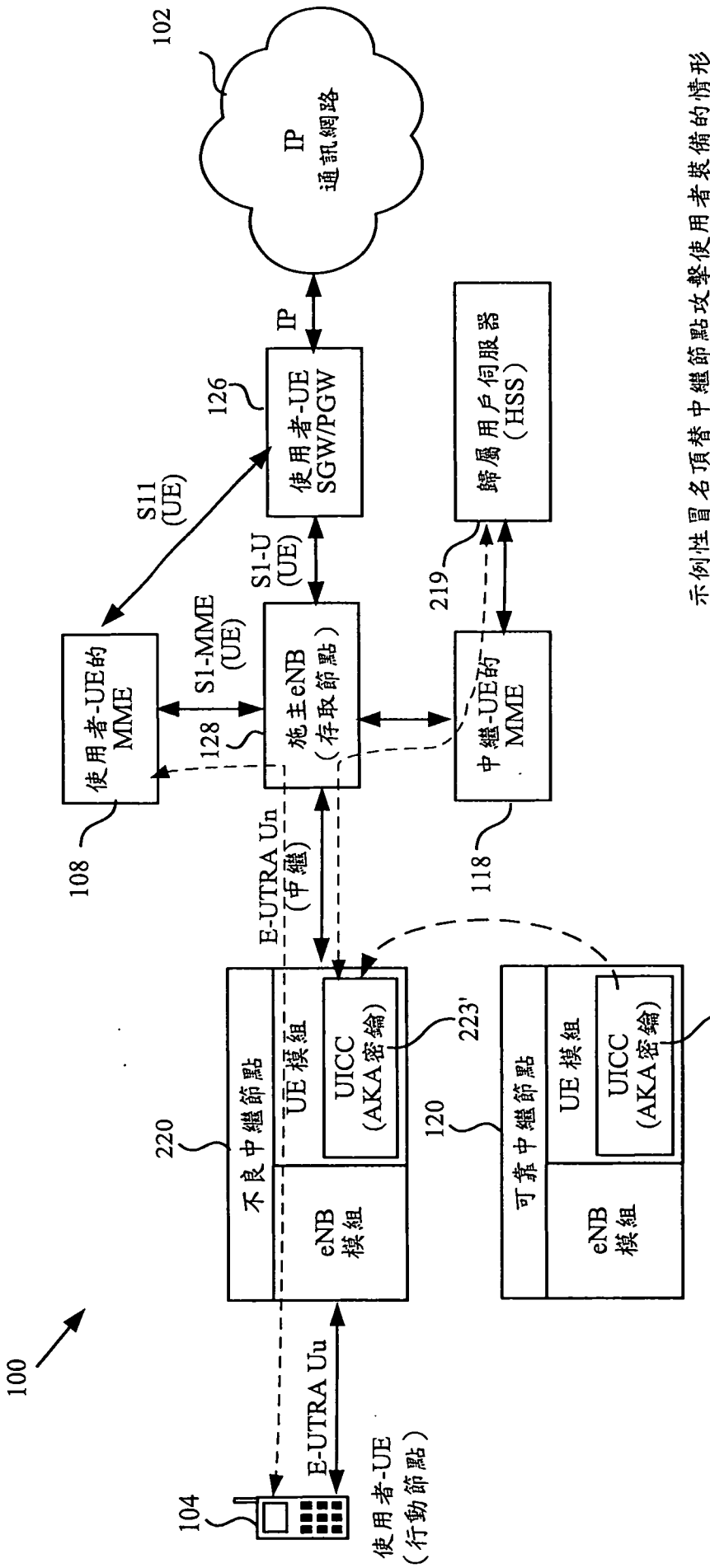


圖2

示例性冒名頂替中繼節點攻擊使用者裝備的情形

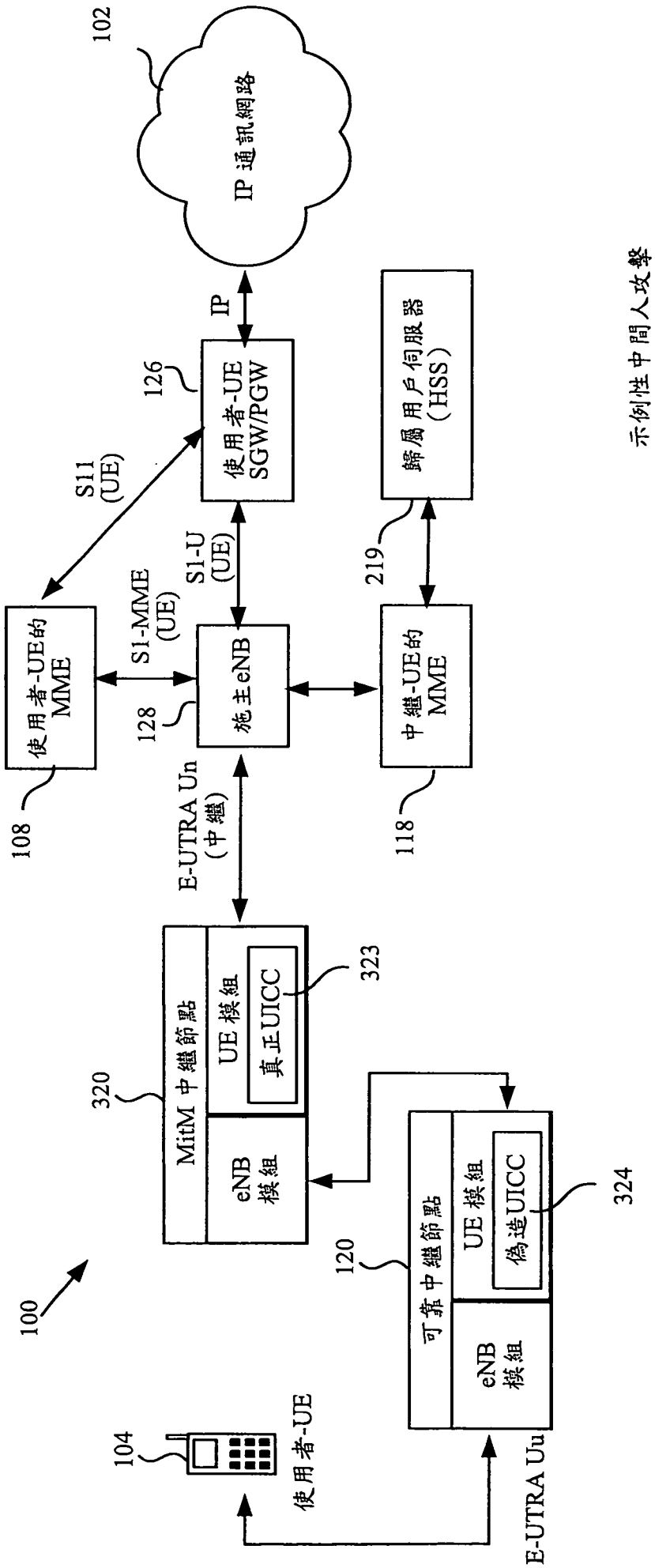

102
IP 通訊網路
IP
126
使用者-UE SGW/PGW
S11 (UE)
S1-U (UE)
S1-MME (UE)
219
歸屬用戶伺服器 (HSS)
使用者-UE的 MME
128
施主eNB
中繼-UE的 MME
108
118
E-UTRA Un (中繼)
320
MitM 中繼節點
UE 模組
真正UICC
323
eNB 模組
100
120
可靠中繼節點
UE 模組
偽造UICC
324
eNB 模組
104
使用者-UE
E-UTRA Uu

圖3 示例性中間人攻擊

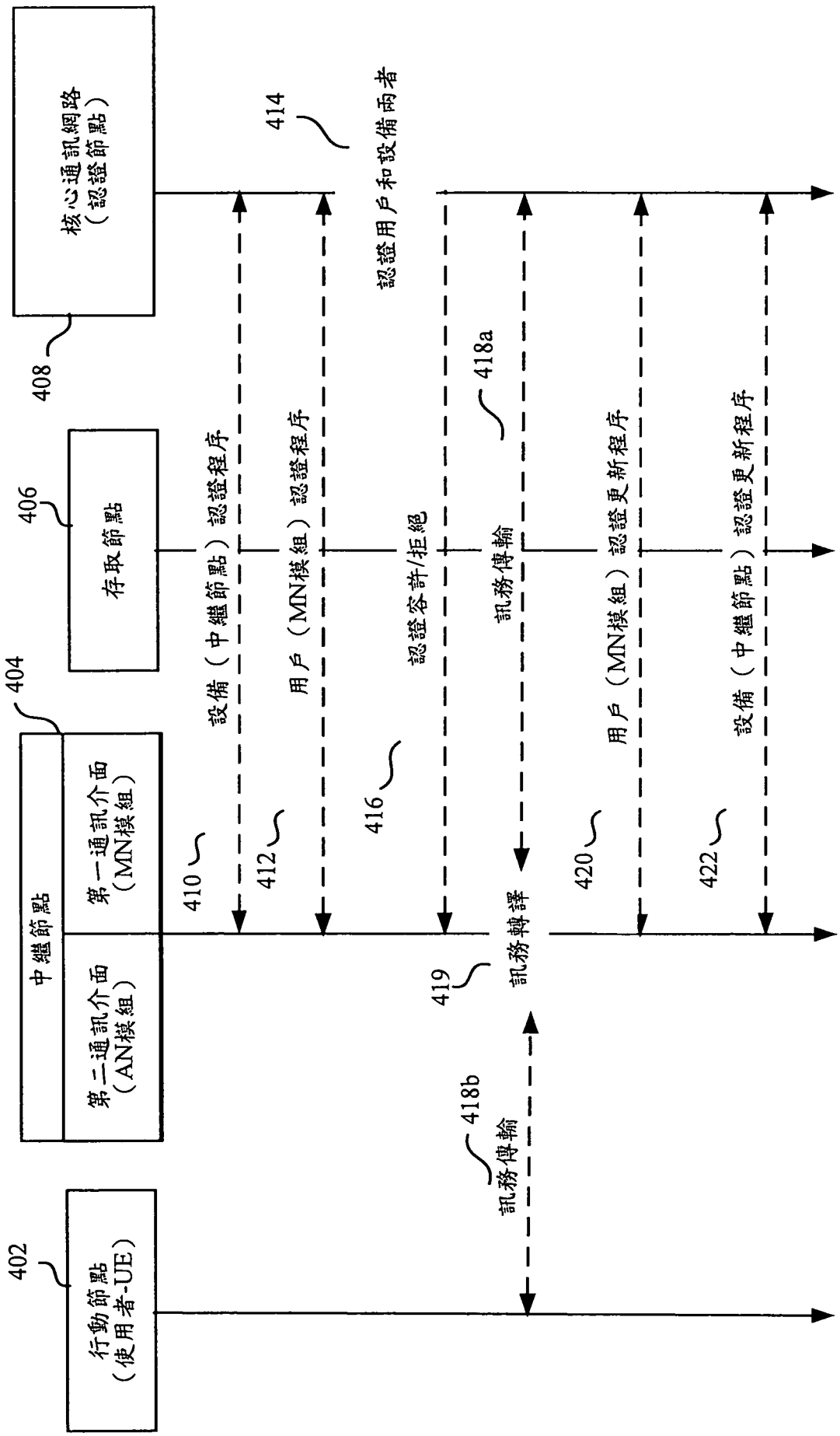

核心通訊網路
（認證節點）
408
414
存取節點
406
認證用戶和設備兩者
404
中繼節點
第一通訊介面
（MN模組）
第二通訊介面
（AN模組）
設備（中繼節點）認證程序
用戶（MN模組）認證程序
410
412
416
認證容許/拒絕
418a
訊務傳輸
420
422
419
訊務轉譯
418b
訊務傳輸
行動節點
（使用者-UE）
402
中繼節點認證方案

圖4

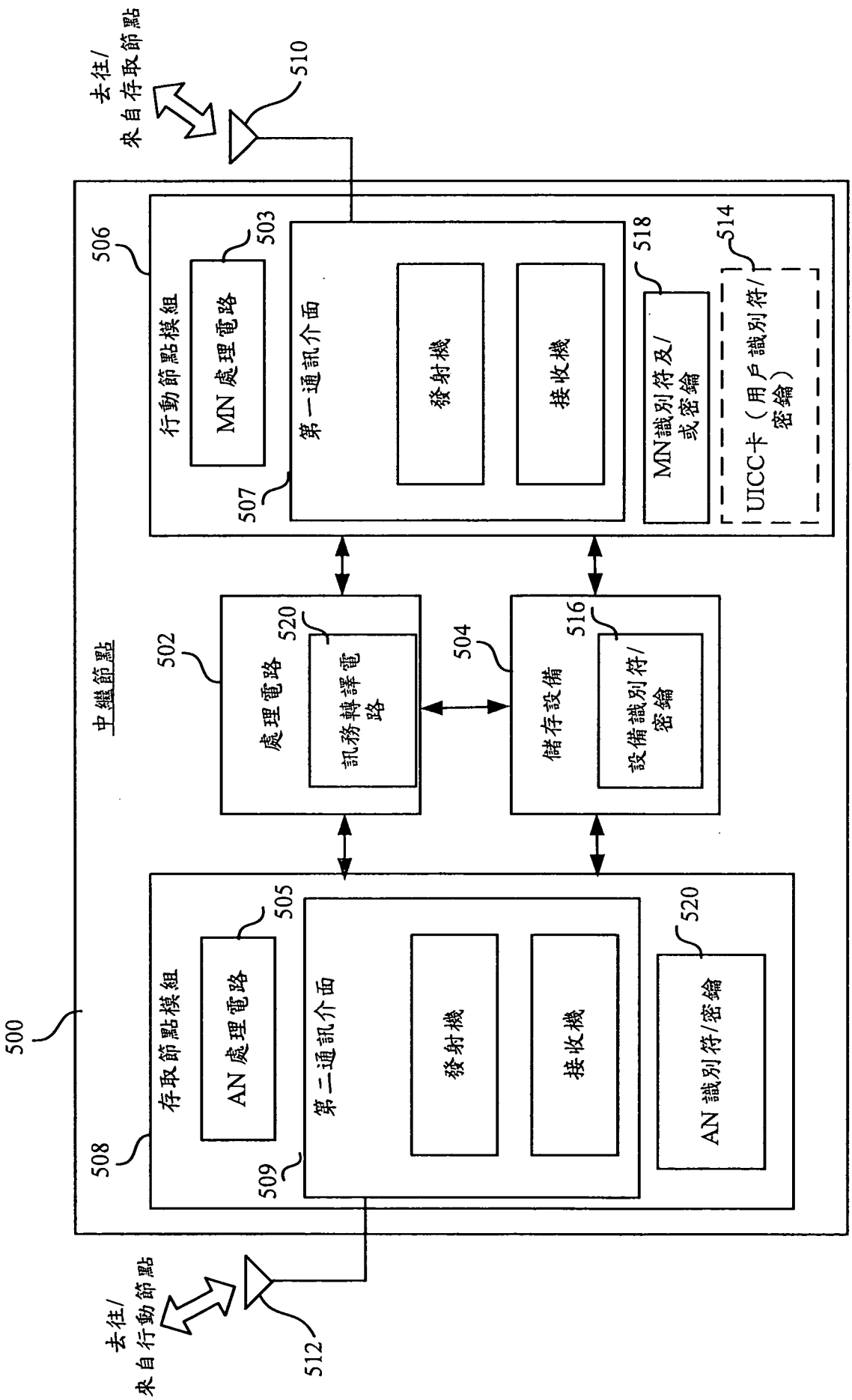

去往/
來自存取節點
510
506
行動節點模組
MN 處理電路
503
第一通訊介面
507
發射機
接收機
518
MN識別符及/
或密鑰
514
UICC卡（用戶識別符/
密鑰）
中繼節點
502
處理電路
520
訊務轉譯電
路
504
儲存設備
516
設備識別符/
密鑰
500
存取節點模組
AN 處理電路
505
第二通訊介面
509
發射機
接收機
520
AN 識別符/密鑰
508
去往/
來自行動節點
512

圖 5

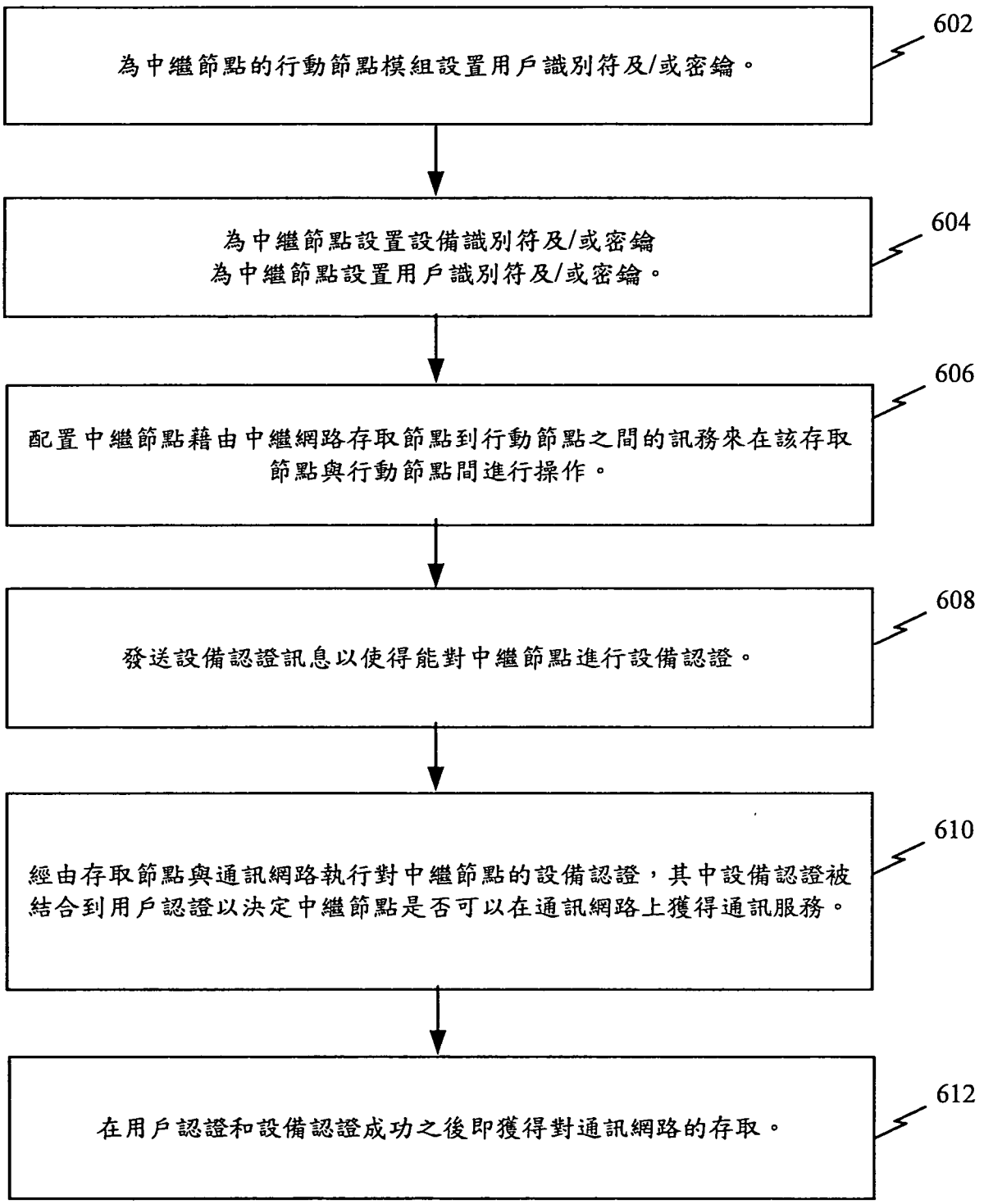

為中繼節點的行動節點模組設置用戶識別符及/或密鑰。
602
為中繼節點設置設備識別符及/或密鑰
為中繼節點設置用戶識別符及/或密鑰。
604
配置中繼節點藉由中繼網路存取節點到行動節點之間的訊務來在該存取節點與行動節點間進行操作。
606
發送設備認證訊息以使得能對中繼節點進行設備認證。
608
經由存取節點與通訊網路執行對中繼節點的設備認證，其中設備認證被結合到用戶認證以決定中繼節點是否可以在通訊網路上獲得通訊服務。
610
在用戶認證和設備認證成功之後即獲得對通訊網路的存取。
612

圖6

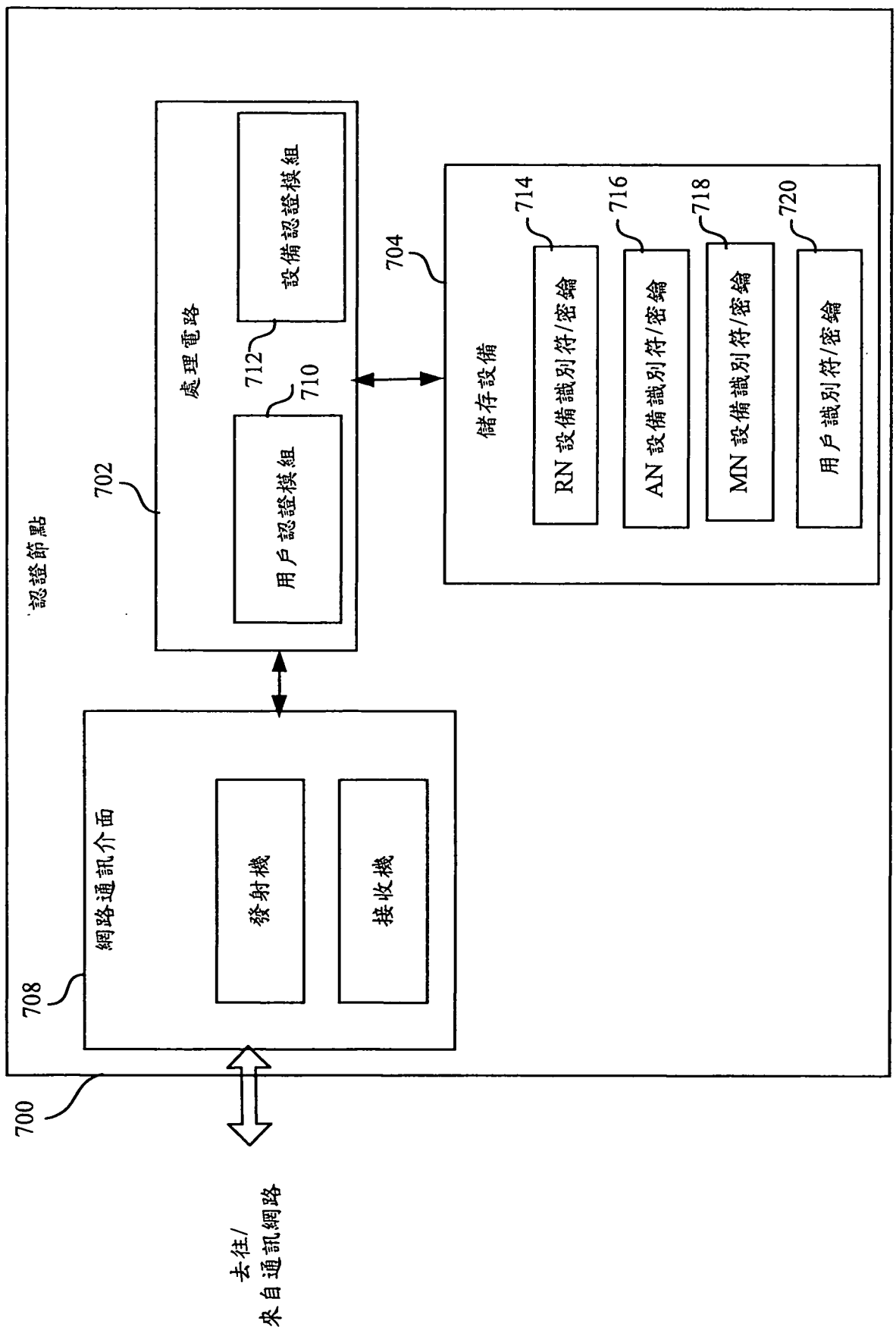

認證節點
700
網路通訊介面
708
發射機
接收機
去往/
來自通訊網路
處理電路
702
用戶認證模組
710
設備認證模組
712
704
儲存設備
RN 設備識別符/密鑰
714
AN 設備識別符/密鑰
716
MN 設備識別符/密鑰
718
用戶識別符/密鑰
720

圖 7

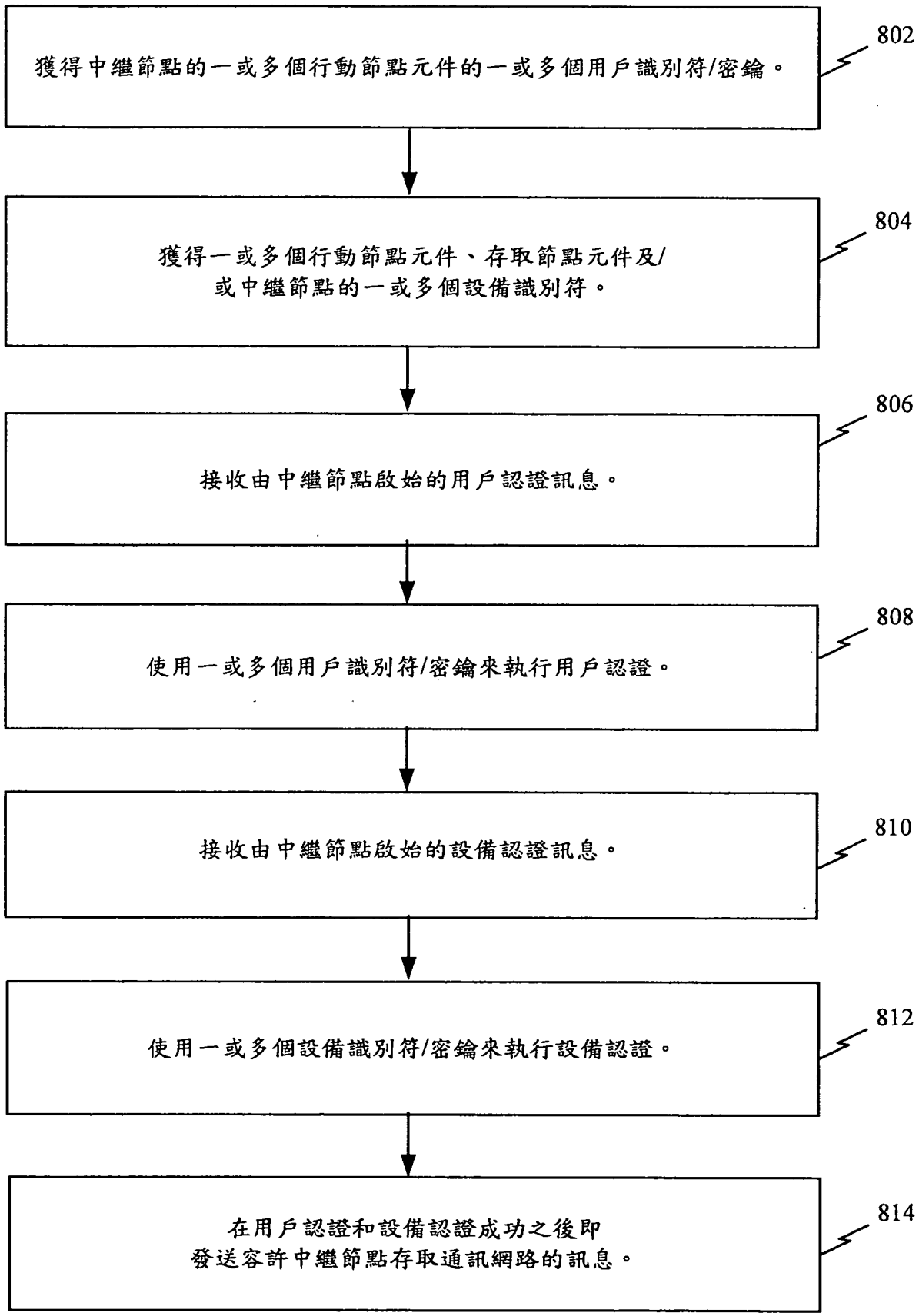

獲得中繼節點的一或多個行動節點元件的一或多個用戶識別符/密鑰。
802
獲得一或多個行動節點元件、存取節點元件及/或中繼節點的一或多個設備識別符。
804
接收由中繼節點啟始的用戶認證訊息。
806
使用一或多個用戶識別符/密鑰來執行用戶認證。
808
接收由中繼節點啟始的設備認證訊息。
810
使用一或多個設備識別符/密鑰來執行設備認證。
812
在用戶認證和設備認證成功之後即發送容許中繼節點存取通訊網路的訊息。
814

圖8