I779106

(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 I779106 B**

(45)公告日： 中華民國 111 (2022) 年 10 月 01 日

(21)申請案號：107134619 (22)申請日： 中華民國 107 (2018) 年 10 月 01 日

(51)Int. Cl.： ***H04L12/58 (2006.01)*** ***H04L9/14 (2006.01)***

(30)優先權：2017/10/02 美國 62/567,086

2018/09/28 美國 16/146,709

(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)；伊史考特 愛德利恩愛德華 ESCOTT, ADRIAN EDWARD (GB)；帕拉尼古德 艾納德 PALANIGOUNDER, ANAND (IN)

(74)代理人：李世章

(56)參考文獻：

TW 201404191A

網路文獻 ZTE, China Unicom, "Key hierarchy for 5G", 3GPP TSG SA WG3 (Security) Meeting #87; S3-171605, 2017/06/05 https://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_87_Ljubljana/Docs/

網路文獻 ZTE, "Update of solution 8.5", 3GPP TSG SA WG3 (Security) Meeting #87; S3-171053, 2017/05/08 https://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_87_Ljubljana/Docs/

審查人員：黎芷婷

申請專利範圍項數：47 項 圖式數：15 共 77 頁

(54)名稱

用於在金鑰產生中合併網路策略的方法、使用者設備及安全錨功能單元

(57)摘要

本案內容提供了可以應用於例如以安全的方式提供網路策略資訊的技術。在一些情況下，UE可以進行以下操作：接收用於與網路建立安全連接的第一訊息，其中第一訊息包括網路策略資訊；部分地基於網路策略資訊來產生第一金鑰；及使用第一金鑰來驗證網路策略資訊。

The present disclosure provides techniques that may be applied, for example, for providing network policy information in a secure manner. In some cases, a UE may receive a first message for establishing a secure connection with a network, wherein the first message comprises network policy information, generate a first key based in part on the network policy information, and use the first key to verify the network policy information.

指定代表圖：

符號簡單說明：

1000:操作

1002:步驟

1004:步驟

1006:步驟

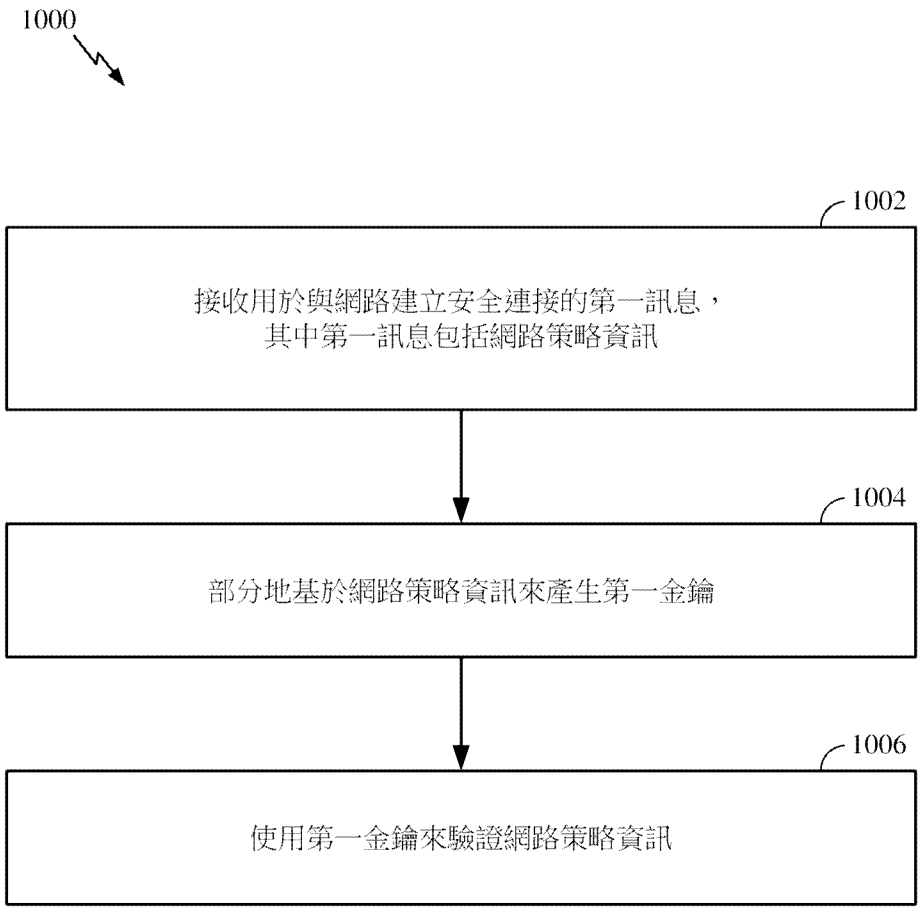

圖10

111年4月15日 所提修正

I779106

【發明摘要】

【中文發明名稱】用於在金鑰產生中合併網路策略的方法、使用者設備及安全錨功能單元

【英文發明名稱】METHOD, USER EQUIPMENT, AND SECURITY ANCHOR FUNCTION FOR INCORPORATING NETWORK POLICIES IN KEY GENERATION

【中文】

本案內容提供了可以應用於例如以安全的方式提供網路策略資訊的技術。在一些情況下，UE可以進行以下操作：接收用於與網路建立安全連接的第一訊息，其中第一訊息包括網路策略資訊；部分地基於網路策略資訊來產生第一金鑰；及使用第一金鑰來驗證網路策略資訊。

【英文】

The present disclosure provides techniques that may be applied, for example, for providing network policy information in a secure manner. In some cases, a UE may receive a first message for establishing a secure connection with a network, wherein the first message comprises network policy information, generate a first key based in part on the network policy information, and use the first key to verify the network policy information.

【指定代表圖】第（ 10 ）圖。

【代表圖之符號簡單說明】

1000 操作

1002 步驟

1004 步驟

1006 步驟

【特徵化學式】

無

【發明說明書】

【中文發明名稱】用於在金鑰產生中合併網路策略的方法、使用者設備及安全錨功能單元

【英文發明名稱】METHOD, USER EQUIPMENT, AND SECURITY ANCHOR FUNCTION FOR INCORPORATING NETWORK POLICIES IN KEY GENERATION

【技術領域】

【0001】 本專利申請案主張享受於2017年10月2日提出申請的美國臨時專利申請第62/567,086號的權益，該臨時專利申請的全部內容以引用的方式併入本文中。

【0002】 概括而言，本案內容的某些態樣涉及無線通訊，並且更具體而言，本案內容的某些態樣涉及用於在網路中建立安全通訊的方法和裝置。

【先前技術】

【0003】 廣泛地部署無線通訊系統以提供各種電信服務，例如，電話、視訊、資料、訊息傳遞和廣播。典型的無線通訊系統可以採用能夠經由共享可用的系統資源(例如，頻寬、發射功率）來支援與多個使用者的通訊的多工存取技術。此種多工存取技術的實例係包括長期進化（LTE）系統、分碼多工存取（CDMA）系統、分時多工存取（TDMA）系統、分頻多工存取（FDMA）系統、正交分頻多工存取（OFDMA）系統、單載波分頻多工存取（SC-FDMA）系統和分時同步分碼多工存取（TD-SCDMA）系統。

【0004】 在一些實例中，無線多工存取通訊系統可以包括多個基地台，每個基地台同時支援針對多個通訊設備

（其另外被稱為使用者設備（UE））的通訊。在LTE或LTE-A網路中，一或多個基地台的集合可以定義進化型節點B（eNB）。在其他實例中（例如，在下一代或5G網路中），無線多工存取通訊系統可以包括與多個中央單元（CU）（例如，中央節點（CN）、存取節點控制器（ANC）等）通訊的多個分散式單元（DU）（例如，邊緣單元（EU）、邊緣節點（EN）、無線電頭端（RH）、智能無線電頭端（SRH）、發送接收點（TRP）等），其中與中央單元通訊的一或多個分散式單元的集合可以定義存取節點（例如，新無線電基地台（NR BS）、新無線電節點B（NR NB）、網路節點、5G NB、gNB等）。基地台或DU可以在下行鏈路通道（例如，用於來自基地台或去往UE的傳輸）和上行鏈路通道（例如，用於從UE到基地台或分散式單元的傳輸）上與UE集合通訊。

【0005】 已經在各種電信標準中採用了該等多工存取技術以提供公共協定，該公共協定使得不同的無線設備能夠在城市、國家、地區以及乃至全球層面上通訊。新興的電信標準的實例是新無線電（NR），例如，5G無線存取。NR是對由第三代合作夥伴計畫（3GPP）頒佈的LTE行動服務標準的增強集。其被設計為經由提高頻譜效率、降低成本、改進服務、利用新頻譜、以及在下行鏈路（DL）上和在上行鏈路（UL）上使用具有循環字首（CP）的OFDMA來與其他開放標準更好地整合，從而更好地支援

行動寬頻網際網路存取，以及支援波束成形、多輸入多輸出（MIMO）天線技術和載波聚合。

【0006】 然而，隨著對行動寬頻存取的需求持續增加，存在對NR技術的進一步改進的需求。優選地，該等改進應該適用於其他多工存取技術和採用該等技術的電信標準。

【發明內容】

【0007】 本案內容的系統、方法和設備均具有數個態樣，其中沒有單個態樣單獨地負責其所期望的屬性。在不限制本案內容的如下文的請求項所表達的範疇的情況下，現在將簡要地論述一些特徵。在考慮了該論述之後，並且特別是在閱讀了標題為「具體實施方式」的小節之後，將理解本案內容的特徵如何提供包括在無線網路中的改進的通訊的優勢。

【0008】 本案內容的某些態樣提供了一種用於由使用者設備（UE）進行無線通訊的方法。概括而言，該方法包括：接收用於與網路建立安全連接的第一訊息，其中第一訊息包括網路策略資訊。該方法亦包括：部分地基於網路策略資訊來產生第一金鑰。該方法亦包括：使用第一金鑰來驗證網路資訊。

【0009】 本案內容的某些態樣提供了一種用於由網路節點（如安全錨功能單元（SEAF））進行無線通訊的方法。概括而言，該方法包括：至少部分地基於網路策略資訊來產生用於網路節點的金鑰。該金鑰用於在UE與網路

節點之間建立安全連接。該方法亦包括：向網路節點發送金鑰。

【0010】 本案內容的某些態樣提供了一種用於由使用者設備（UE）進行無線通訊的方法。概括而言，該方法包括：基於與網路的認證程序來建立UE與網路中的安全錨功能單元（SEAF）之間共享的錨金鑰。該方法亦包括：接收用於與網路建立安全連接的第一訊息，其中第一訊息包括用於與網路的通訊通信期的網路策略符記、網路策略資訊、第一金鑰有效的第一時間量和網路策略符記有效的第二時間量。該方法亦包括：在與網路建立安全連接之前，基於從所共享的錨金鑰、網路策略資訊、第一時間量和第二時間量推導出的金鑰來決定網路策略符記是否是有效的。

【0011】 本案內容的某些態樣提供了一種用於由網路節點（如安全錨功能單元（SEAF））進行無線通訊的方法。概括而言，該方法包括：基於與UE的認證程序來建立在網路中在SEAF與UE之間共享的錨金鑰。該方法亦包括：部分地基於錨金鑰、網路策略資訊和網路策略符記有效的第一時間量來產生網路策略符記。該方法亦包括：產生用於另一網路節點的金鑰；及向另一網路節點發送金鑰、網路策略資訊和網路策略符記。

【0012】 提供了包括能夠執行上文所描述的操作的方法、裝置、系統、電腦程式產品和處理系統的數個其他態樣。

【0013】 為了實現前述目的和相關目的，一或多個態樣包括下文中充分描述的特徵以及在申請專利範圍中特別指出的特徵。下文的描述和附圖詳細闡述了一或多個態樣的某些說明性的特徵。然而，該等特徵表明可以使用各態樣的原理的各種方式中的僅一些方式，以及該描述意欲包括全部此種態樣和其均等物。

【圖式簡單說明】

【0014】 為了可以詳細地理解本案內容的上述特徵，可以經由參考各態樣獲得上文簡要概述的更具體的描述，該態樣中的一些態樣在附圖中示出。然而，要注意的是，附圖僅圖示本案內容的某些典型的態樣，並且因此不應被視為限制其範疇，因為該描述可以容許其他同等有效的態樣。

【0015】 圖1是概念性地示出根據本案內容的某些態樣的示例性電信系統的方塊圖。

【0016】 圖2是示出根據本案內容的某些態樣的分散式RAN的示例性邏輯架構的方塊圖。

【0017】 圖3是示出根據本案內容的某些態樣的分散式RAN的示例性實體架構的圖。

【0018】 圖4是概念性地示出根據本案內容的某些態樣的示例性BS和使用者設備（UE）的設計的方塊圖。

【0019】 圖5是示出根據本案內容的某些態樣的用於實現通訊協定堆疊的實例的圖。

【0020】 圖6示出根據本案內容的某些態樣的以DL為中心的子訊框的實例。

【0021】 圖7示出根據本案內容的某些態樣的以UL為中心的子訊框的實例。

【0022】 圖8-9示出根據本案內容的某些態樣的具有一或多個非共置網路節點的示例性5G架構。

【0023】 圖10是示出根據本案內容的某些態樣的用於網路中的無線通訊的示例性操作的流程圖。

【0024】 圖11是示出根據本案內容的某些態樣的用於網路中的無線通訊的示例性操作的流程圖。

【0025】 圖12是示出根據本案內容的某些態樣的示例性註冊程序的撥叫流程圖。

【0026】 圖13是示出根據本案內容的某些態樣的用於網路中的無線通訊的示例性操作的流程圖。

【0027】 圖14是示出根據本案內容的某些態樣的用於網路中的無線通訊的示例性操作的流程圖。

【0028】 圖15是示出根據本案內容的某些態樣的示例性註冊程序的撥叫流程圖。

【0029】 為了有助於理解，在可能的情況下，已經使用相同的元件符號來代表對於該等圖而言共同的相同元件。預期的是，在一個實施例中所揭示的元素可以有利地用於其他實施例上，而無需具體記載。

【實施方式】

【0030】 本案內容的各態樣提供了用於無線網路(如新無線電(NR)(新無線電存取技術或5G技術)無線網路)的裝置、方法、處理系統和電腦可讀取媒體。

【0031】 NR可以支援各種無線通訊服務，例如，以寬頻寬(例如，80 MHz以上)為目標的增強型行動寬頻(eMBB)、以高載波頻率(例如，60 GHz)為目標的毫米波(mmW)、以非向後相容MTC技術為目標的大容量MTC(mMTC)及/或以超可靠低延時通訊(URLLC)為目標的任務關鍵。該等服務可以包括延時和可靠性要求。該等服務亦可以具有不同的傳輸時間間隔(TTI)，以滿足各自的服務品質(QoS)要求。此外，該等服務可以共存於同一子訊框中。

【0032】 NR引入了網路切分(network slicing)的概念。例如，網路可以具有多個切片，該多個切片可以支援不同的服務(例如，萬聯網路(IoE)、URLLC、eMBB、車輛到車輛(V2V)通訊等)。切片可以被定義為完整的邏輯網路，其包括網路功能的集合以及用於提供某些網路能力和網路特性所必需的相應資源。

【0033】 在一些態樣中，5G NR系統能夠支援各種不同的部署場景。具體而言，隨著5G技術及/或服務要求不斷進化，由5G網路中的一或多個網路節點執行的服務、能力及/或功能可以改變。由於UE可能不知道網路架構中的變化，因此向UE通知特定的網路配置、能力、安全配置等可能是有益的。然而，使用當前技術來使網路以安全

的方式向UE通知關於網路（安全）配置、能力和策略，此可能是不太可能的。

【0034】 例如，在5G系統中，在UE與服務網路之間通常存在單個控制平面介面（N1）。該N1介面通常用於在UE與存取和行動性管理功能單元（AMF）AMF之間建立非存取層（NAS）連接。然而，在一些部署場景中，AMF可能不負責網路中的安全功能（或者可能無權限用網路中的安全功能）。因此，由於AMF可能是具有與UE的信號傳遞連接的唯一實體，所以可能存在(欺詐或惡意）AMF可以攔截網路配置資訊並且修改被提供給UE的網路配置資訊以危害UE與網路之間的連接/通訊的情況。因此，本案內容的各態樣提供了用於向UE安全地通知關於網路（安全）配置、能力、網路策略等的技術。

【0035】 在下文中參考附圖更充分地描述了本案內容的各個態樣。然而，本案內容可以以諸多不同的形式體現，並且不應當被解釋為限於本案全篇提供的任何特定結構或功能。確切而言，提供該等態樣是為了本案內容將是透徹並且完整的，以及該等態樣將向本領域技藝人士充分地傳達本案內容的範疇。基於本文的教導，本領域技藝人士應當理解，本案內容的範疇意欲涵蓋本文所揭示的本案內容的任何態樣，無論該態樣是獨立本案內容的任何其他態樣來實現的還是與本案內容的任何其他態樣相結合來實現的。例如，使用本文闡述的任何數量的態樣，可以實現一種裝置或者可以實施一種方法。另外，本案內容的範

嚐意欲涵蓋使用除了本文所闡述的本案內容的各個態樣之外或與其不同的其他結構、功能或者結構和功能來實施的此種裝置或方法。應當理解的是，本文所揭示的本案內容的任何態樣可以經由請求項的一或多個要素來體現。

【0036】 本文使用「示例性」一詞意指「用作示例、實例或說明」。本文中被描述為「示例性」的任何態樣未必被解釋為相對於其他態樣優選或具有優勢。

【0037】 儘管本文描述了特定態樣，但是該等態樣的諸多變化和置換符合本案內容的範嚐。儘管提到了優選態樣的一些益處和優點，但是本案內容的範圍並不意欲限於特定的益處、用途或目的。確切而言，本案內容的各態樣意欲廣泛地適用於不同的無線技術、系統配置、網路和傳輸協定，其中一些在附圖中以及在對優選態樣的以下描述中經由距離的方式進行說明。詳細描述和附圖僅是對本案內容進行說明而不是限制，本案內容的範嚐由所附請求項及其均等物限定。

【0038】 本文中所描述的技術可以用於各種無線通訊網路，諸如CDMA、TDMA、FDMA、OFDMA、SC-FDMA和其他網路。術語「網路」和「系統」經常互換使用。CDMA網路可以實現諸如通用陸地無線存取（UTRA）、cdma2000等的無線電技術。UTRA包括寬頻CDMA（WCDMA）、時分同步CDMA（TD-SCDMA）和CDMA的其他變型。cdma2000涵蓋IS-2000、IS-95和IS-856標準。TDMA網路可以實

現諸如行動通訊全球系統（GSM）之類的無線電技術。OFDMA網路可以實現諸如進化型UTRA（E-UTRA）、超行動寬頻（UMB）、IEEE 802.11（Wi-Fi）、IEEE 802.16（WiMAX）、IEEE 802.20、快閃OFDM®等的無線電技術。UTRA和E-UTRA是通用行動電信系統（UMTS）的一部分。在分頻雙工（FDD）和分時雙工（TDD）兩者中，3GPP長期進化（LTE）和改進的LTE（LTE-A）是UMTS的使用E-UTRA的新版本，其在下行鏈路上採用OFDMA以及在上行鏈路上採用SC-FDMA。在來自名稱為「第三代合作夥伴計畫」（3GPP）的組織的文件中描述了UTRA、E-UTRA、UMTS、LTE、LTE-A和GSM。在來自名稱為「第三代合作夥伴計畫2」（3GPP2）的組織的文件中描述了cdma2000和UMB。本文中所描述的技術可以用於上文提及的無線網路和無線電技術以及其他無線網路和無線電技術（諸如5G下一代/NR網路）。

示例性無線通訊系統

【0039】 圖1圖示示例性無線網路100（如新無線電（NR）或5G網路），在無線網路100中，可以執行本案內容的各態樣，例如以用於向UE安全地提供網路（安全）策略資訊（例如，網路配置、安全資訊、能力等）。在一些情況下，網路100可以是多切片網路，其中每個切片定義為被附隨在一起以滿足特定用例或傳輸量模型的要求

的充分配置的網路功能、網路應用和底層雲基礎設施的組成。

【0040】 如在圖1中所示出的，無線網路100可以包括多個BS 110和其他網路實體。BS可以是與UE通訊的站。每個BS 110可以為特定地理區域提供通訊覆蓋。在3GPP中，術語「細胞」可以指的是節點B的覆蓋區域及/或服務於該覆蓋區域的節點B子系統，此取決於使用該術語的上下文。在NR系統中，術語「細胞」和eNB、節點B、5G NB、AP、NR BS、NR BS或TRP可以互換。在一些實例中，細胞可能未必是靜止的，以及細胞的地理區域可以根據行動基地台的位置來移動。在一些實例中，基地台可以經由各種類型的回載介面（例如，直接實體連接、虛擬網路或者使用任何適當的傳輸網路的類似介面）彼此互連及/或互連到無線網路100中的一或多個其他基地台或網路節點（未圖示）。

【0041】 通常，在給定的地理區域中可以部署任何數量的無線網路。每個無線網路可以支援特定的無線電存取技術（RAT），並且可以在一或多個頻率上操作。RAT亦可以被稱為無線電技術、空中介面等。頻率亦可以被稱為載波、頻率通道等。每個頻率可以在給定的地理區域中支援單個RAT，以便避免在不同的RAT的無線網路之間的干擾。在一些情況下，可以部署採用多切片網路架構的NR或者5G RAT網路。

【0042】 BS可以為巨集細胞、微微細胞、毫微微細胞及/或其他類型的細胞提供通訊覆蓋。巨集細胞可以覆蓋相對大的地理區域（例如，半徑為數公里），並且可以允許由具有服務訂製的UE進行的不受限制的存取。微微細胞可以覆蓋相對小的地理區域，並且可以允許由具有服務訂製的UE進行的不受限制的存取。毫微微細胞可以覆蓋相對小的地理區域（例如，住宅），並且可以允許由與毫微微細胞具有關聯的UE（例如，在封閉使用者群組（CSG）中的UE、針對在住宅中的使用者的UE等）進行的受限制的存取。用於巨集細胞的BS可以被稱為巨集BS。用於微微細胞的BS可以被稱為微微BS。用於毫微微細胞的BS可以被稱為毫微微BS或家庭BS。在圖1中所示出的實例中，BS 110a、110b和110c可以分別是用於巨集細胞102a、102b和102c的巨集BS。BS 110x可以是用於微微細胞102x的微微BS。BS 110y和110z可以分別是用於毫微微細胞102y和102z的毫微微BS。BS可以支援一或多個（例如，三個）細胞。

【0043】 無線網路100亦可以包括中繼站。中繼站是從上游站（例如，BS或UE）接收資料及/或其他資訊的傳輸以及向下游站（例如，UE或BS）發送資料及/或其他資訊的傳輸的站。中繼站亦可以是為其他UE中繼傳輸的UE。在圖1中所示出的實例中，中繼站110r可以與BS 110a和UE 120r通訊，以便促進在BS 110a與UE 120r之間的通訊。中繼站亦可以被稱為中繼BS、中繼器等。

【0044】 無線網路100可以是包括不同類型的BS（例如，巨集BS、微微BS、毫微微BS、中繼器等）的異質網路。該等不同類型的BS可以具有不同的發射功率位準、不同的覆蓋區域以及對無線網路100中的干擾的不同影響。例如，巨集BS可以具有高發射功率位準（例如，20瓦），而微微BS、毫微微BS和中繼器可以具有較低的發射功率位準（例如，1瓦）。

【0045】 無線網路100可以支援同步操作或非同步操作。對於同步操作而言，BS可以具有類似的訊框時序，以及來自不同BS的傳輸可以在時間上近似對準。對於非同步操作而言，BS可以具有不同的訊框時序，以及來自不同BS的傳輸可能在時間上不對準。本文中描述的技術可以用於同步操作和非同步操作兩者。

【0046】 網路控制器130可以耦合到BS的集合，並且提供針對該等BS的協調和控制。網路控制器130可以經由回載與BS 110通訊。BS 110亦可以例如經由無線或有線回載來直接地或間接地彼此進行通訊。

【0047】 UE 120（例如，120x、120y等）可以散佈在整個無線網路100中，並且每個UE可以是靜止的或者移動的。UE亦可以被稱為行動站、終端、存取終端、使用者單元、站、客戶駐地設備（CPE）、蜂巢式電話、智慧型電話、個人數位助理（PDA）、無線數據機、無線通訊設備、手持設備、膝上型電腦、無線電話、無線區域迴路（WLL）站、平板設備、照相機、遊戲裝置、小

筆電、智慧型電腦、超級本、醫療設備或者醫療裝置、生物感測器/設備、可穿戴設備（例如，智慧手錶、智慧服裝、智慧眼鏡、智慧腕帶、智慧珠寶（例如，智慧指環、智慧手環等））、娛樂設備（例如，音樂設備、視訊設備、衛星無線電單元等）、車輛部件或者感測器、智慧型儀器表/感測器、工業製造設備、全球定位系統設備，或者被配置為經由無線媒體或有線媒體來通訊的任何其他適當的設備。一些UE可以被認為是進化型或者機器類型通訊（MTC）設備或進化型MTC（eMTC）設備。MTC和eMTC UE包括例如機器人、無人機、遠端設備、感測器、儀錶、監控器、位置標籤等，其可以與BS、另一設備（例如，遠端設備）或某種其他實體進行通訊。例如，無線節點可以經由有線或無線通訊鏈路提供針對網路（例如，如網際網路或蜂巢網路之類的廣域網）的連接或者到網路的連接。一些UE可以被認為是物聯網路（IoT）設備。

【0048】 在圖1中，具有雙箭頭的實線指示在UE與服務BS之間的期望傳輸，服務BS是被指定為在下行鏈路及/或上行鏈路上為UE服務的BS。具有雙箭頭的虛線指示在UE與BS之間的干擾傳輸。

【0049】 某些無線網路（例如，LTE）在下行鏈路上利用正交分頻多工（OFDM），以及在上行鏈路上利用單載波分頻多工（SC-FDM）。OFDM和SC-FDM將系統頻寬劃分成多個（K）正交次載波，其通常亦被稱為音調、頻段等。可以利用資料來調變每個次載波。通常，調

變符號是在頻域中利用OFDM並且在時域中利用SC-FDM來發送的。在相鄰次載波之間的間隔可以是固定的，以及次載波的總數（K）可以取決於系統頻寬。例如，次載波的間隔可以是15 kHz，以及最小資源配置（被稱為「資源區塊」）可以是12個次載波（或180 kHz）。因此，對於1.25、2.5、5、10或20兆赫（MHz）的系統頻寬而言，標稱的FFT大小可以分別等於128、256、512、1024或2048。系統頻寬亦可以被劃分成次頻帶。例如，次頻帶可以覆蓋1.08 MHz（亦即，6個資源區塊），並且對於1.25、2.5、5、10或20 MHz的系統頻寬而言，可以分別存在1、2、4、8或16個次頻帶。

【0050】 儘管本文中所描述的實例的各態樣可以與LTE技術相關聯，但是本案內容的各態樣可以適用於其他無線通訊系統，如NR/5G。

【0051】 NR可以在上行鏈路和下行鏈路上利用具有CP的OFDM，並且包括對使用TDD的半雙工操作的支援。可以支援100 MHz的單分量載波頻寬。NR資源區塊可以在0.1 ms持續時間內跨越具有75 kHz的次載波頻寬的12個次載波。每個無線訊框可以包括具有10 ms長度的50個子訊框。因此，每個子訊框可以具有0.2ms的長度。每個子訊框可以指示用於資料傳輸的鏈路方向（亦即，DL或UL），並且針對每個子訊框的鏈路方向可以動態地切換。每個子訊框可以包括DL/UL資料以及DL/UL控制資料。用於NR的UL和DL子訊框可以如下文

關於圖6和圖7更詳細地描述的。可以支援波束成形，並且可以動態地配置波束方向。亦可以支援具有預編碼的MIMO傳輸。在DL中的MIMO配置可以支援多達8個發射天線，其中多層DL傳輸多達8個串流，以及每UE多達2個串流。可以支援具有每UE多達2個串流的多層傳輸。可以支援具有多達8個服務細胞的多個細胞的聚合。替代地，NR可以支援除了基於OFDM的空中介面之外的不同的空中介面。NR網路可以包括諸如CU及/或DU之類的實體。

【0052】 在一些實例中，可以排程對空中介面的存取，其中排程實體（例如，基地台）在其服務區域或細胞內的一些或所有設備和裝置之間分配用於通訊的資源。在本案內容中，如下文進一步論述的，排程實體可以負責排程、指派、重新配置和釋放用於一或多個從屬實體的資源。亦即，對於所排程的通訊而言，從屬實體利用由排程實體分配的資源。基地台不是可以用作排程實體的唯一實體。亦即，在一些實例中，UE可以用作排程實體，其排程用於一或多個從屬實體（例如，一或多個其他UE）的資源。在該實例中，該UE正在用作排程實體，而其他UE利用由該UE排程的資源進行無線通訊。UE可以在同級間（P2P）網路中及/或在網狀網路中用作排程實體。在網狀網路實例中，除了與排程實體進行通訊之外，UE亦可以可選性地彼此直接通訊。

【0053】 因此，在具有對時間-頻率資源的排程存取並且具有蜂巢配置、P2P配置和網狀配置的無線通訊網路中，排程實體和一或多個從屬實體可以利用所排程的資源進行通訊。

【0054】 如前述，RAN可以包括CU和DU。NR BS（例如，gNB、5G節點B、節點B、發送接收點（TRP）、存取點（AP））可以對應於一或多個BS。NR細胞可以被配置為存取細胞（ACell）或僅資料細胞（DCell）。例如，RAN（例如，中央單元或分散式單元）可以配置細胞。DCell可以是用於載波聚合或雙連接的細胞，但是不用於初始存取、細胞選擇/重選或交遞。在一些情況下，DCell可以不發送同步信號，在一些情況下，DCell可以發送SS。NR BS可以將用於指示細胞類型的下行鏈路信號發送給UE。基於細胞類型指示，UE可以與NR BS進行通訊。例如，UE可以基於所指示的細胞類型，來決定要考慮細胞選擇、存取、交遞及/或量測的NR BS。

【0055】 圖2圖示可以在圖1中所示出的無線通訊系統中實現的分散式無線電存取網路（RAN）200的示例性邏輯架構。5G存取節點206可以包括存取節點控制器（ANC）202。ANC可以是分散式RAN 200的中央單元（CU）。到下一代核心網路（NG-CN）204的回載介面可以終止於ANC處。到相鄰的下一代存取節點（NG-AN）的回載介面可以終止於ANC處。ANC可以包括一或多個TRP 208（其亦可以被稱為BS、NR BS、

節點B、5G NB、AP，或某種其他術語）。如上文所描述的，TRP可以與「細胞」互換使用。

【0056】 TRP 208可以是DU。TRP可以連接到一個ANC（ANC 202）或者一個以上的ANC（未圖示）。例如，對於RAN共享、無線電即服務（RaaS）和服務特定AND部署而言，TRP可以連接到一個以上的ANC。TRP可以包括一或多個天線埠。TRP可以被配置為單獨地（例如，動態選擇）或者聯合地（例如，聯合傳輸）為UE提供訊務。

【0057】 本端架構200可以用於說明前傳定義。該架構可以被定義為支援跨越不同的部署類型的前傳解決方案。例如，該架構可以是基於發送網路能力（例如，頻寬、延時及/或信號干擾）的。

【0058】 該架構可以與LTE共享特徵及/或部件。根據各態樣，下一代AN（NG-AN）210可以支援與NR的雙連接。NG-AN可以共享用於LTE和NR的公共前傳。

【0059】 該架構可以賦能在TRP 208之間和在TRP 208之中的協調。例如，可以在TRP內及/或經由ANC 202跨越TRP來預先設置協調。根據各態樣，可以不需要/不存在TRP間介面。

【0060】 根據各態樣，拆分邏輯功能的動態配置可以存在於架構200內。如將參考圖5更詳細地描述的，無線電資源控制（RRC）層、封包資料彙聚協定（PDCP）層、無線電鏈路控制（RLC）層、媒體存取控制（MAC）層

和實體（PHY）層可以適應性地置於DU或CU（例如，分別於TRP或ANC）處。根據某些態樣，BS可以包括中央單元（CU）（例如，ANC 202）及/或一或多個分散式單元（例如，一或多個TRP 208）。

【0061】 圖3示出根據本案內容的各態樣的分散式RAN 300的示例性實體架構。集中式核心網路單元（C-CU）302可以主管核心網路功能。C-CU可以是集中地部署的。C-CU功能可以被卸載（例如，至高級無線服務（AWS））以處理峰值容量。

【0062】 集中式RAN單元（C-RU）304可以主管一或多個ANC功能。可選地，C-RU可以在本端主管核心網路功能。C-RU可以具有分散式部署。C-RU可以更接近網路邊緣。

【0063】 DU 306可以主管一或多個TRP（邊緣節點（EN）、邊緣單元（EU）、無線電頭端（RH）、智能無線電頭端（SRH）等）。DU可以位於具有射頻（RF）功能的網路的邊緣。

【0064】 圖4圖示在圖1中所示出的BS 110和UE 120的示例性部件，其可以用於實現本案內容的各態樣。如上文所描述的，BS可以包括TRP。BS 110和UE 120的一或多個部件可以用於實施本案內容的各態樣。例如，UE 120的天線452、Tx/Rx 222、處理器466、458、464及/或控制器/處理器480及/或BS 110的天線434、處理器460、420、438及/或控制器/處理器440

可以用於執行本文所描述的並且參考圖10-圖15所示出的操作。

【0065】 根據各態樣，對於受限的關聯場景而言，基地台110可以是圖1中的巨集BS 110c，以及UE 120可以是UE 120y。基地台110亦可以是某種其他類型的基地台。基地台110可以配備有天線434a至434t，以及UE 120可以配備有天線452a至452r。

【0066】 在基地台110處，發送處理器420可以從資料來源412接收資料，並且從控制器/處理器440接收控制資訊。控制資訊可以用於實體廣播通道（PBCH）、實體控制格式指示符通道（PCFICH）、實體混合ARQ指示符通道（PHICH）、實體下行鏈路控制通道（PDCCH）等。資料可以用於實體下行鏈路共享通道（PDSCH）等。處理器420可以處理（例如，編碼和符號映射）資料和控制資訊，以分別獲得資料符號和控制符號。處理器420亦可以產生參考符號，例如，用於PSS、SSS和細胞特定參考信號。若適用的話，發送（TX）多輸入多輸出（MIMO）處理器430可以對資料符號、控制符號及/或參考符號執行空間處理（例如，預編碼），並且可以向調變器（MOD）432a至432t提供輸出符號串流。每個調變器432可以處理各自的輸出符號串流（例如，用於OFDM等），以獲得輸出取樣串流。每個調變器432可以進一步處理（例如，變換成模擬、放大、濾波和升頻轉換）輸出取樣串流，

以獲得下行鏈路信號。可以分別經由天線434a至434t來發送來自調變器432a至432t的下行鏈路信號。

【0067】 在UE 120處，天線452a至452r可以從基地台110接收下行鏈路信號，並且可以分別向解調器（DEMOD）454a至454r提供接收的信號。每個解調器454可以對各自接收的信號進行調節（例如，濾波、放大、降頻轉換和數位化），以獲得輸入取樣。每個解調器454可以進一步處理輸入取樣（例如，用於OFDM等）以獲得接收符號。MIMO偵測器456可以從所有解調器454a至454r獲得接收符號，對接收符號執行MIMO偵測（若適用），並且提供偵測到的符號。接收處理器458可以處理（例如，解調、解交錯和解碼）偵測到的符號，將針對UE 120的經解碼的資料提供給資料槽460，以及將經解碼的控制資訊提供給控制器/處理器480。

【0068】 在上行鏈路上，在UE 120處，發送處理器464可以接收和處理來自資料來源462的資料（例如，用於實體上行鏈路共享通道（PUSCH））以及來自控制器/處理器480的控制資訊（例如，用於實體上行鏈路控制通道（PUCCH））。發送處理器464亦可以產生針對參考信號的參考符號。若適用的話，來自發送處理器464的符號可以由TX MIMO處理器466來預編碼，由解調器454a至454r進一步處理（例如，用於SC-FDM等），並且被發送給基地台110。在BS 110處，來自UE 120的上行鏈路信號可以由天線434接收，由調變器432處理，由

MIMO偵測器436偵測（若適用的話），並且由接收處理器438進一步處理，以獲得由UE 120發送的經解碼的資料和控制資訊。接收處理器438可以將經解碼的資料提供給資料槽439並且將經解碼的控制資訊提供給控制器/處理器440。

【0069】 控制器/處理器440和480可以分別指導在基地台110和UE 120處的操作。處理器440及/或基地台110處的其他處理器和模組可以執行或指導例如用於本文所描述的技術的程序。處理器480及/或UE 120處的其他處理器和模組亦可以執行或指導例如對在圖10、圖12-圖13及/或圖15中所示出的功能方塊及/或用於本文所描述的技術的其他程序的執行。記憶體442和482可以分別儲存用於BS 110和UE 120的資料和程式碼。排程器444可以排程UE用於在下行鏈路及/或上行鏈路上進行資料傳輸。

【0070】 圖5示出圖示根據本案內容的各態樣的用於實現通訊協定堆疊的實例的圖500。所示出的通訊協定堆疊可以由在5G系統（例如，支援基於上行鏈路的行動性的系統）中操作的設備來實現。圖500示出包括無線電資源控制（RRC）層510、封包資料彙聚協定（PDCP）層515、無線電鏈路控制（RLC）層520、媒體存取控制（MAC）層525和實體（PHY）層530的通訊協定堆疊。在各個實例中，協定堆疊的各層可以被實現為單獨的軟體模組、處理器或ASIC的部分、經由通訊鏈路連接的非共

置設備的部分，或其各種組合。例如，共置的和非共置的實現方式可以用於針對網路存取設備（例如，AN、CU及/或DU）或UE的協定堆疊中。

【0071】 第一選項505-a示出協定堆疊的拆分實現，其中協定堆疊的實現是在集中式網路存取設備（例如，在圖2中的ANC 202）與分散式網路存取設備（例如，在圖2中的DU 208）之間拆分的。在第一選項505-a中，RRC層510和PDCP層515可以由中央單元來實現，以及RLC層520、MAC層525和PHY層530可以由DU來實現。在各個實例中，CU和DU可以是共置或非共置的。第一選項505-a可能在巨集細胞、微細胞或微微細胞部署中是有用的。

【0072】 第二選項505-b示出協定堆疊的統一實現，其中協定堆疊是在單個網路存取設備（例如，存取節點（AN）、新無線電基地台（NR BS）、新無線電節點B（NR NB）、網路節點（NN）等）中實現的。在第二選項中，RRC層510、PDCP層515、RLC層520、MAC層525和PHY層530可以均由AN來實現。第二選項505-b可能在毫微微細胞部署中是有用的。

【0073】 不管網路存取設備是實現協定堆疊的部分還是全部，UE皆可以實現整個協定堆疊（例如，RRC層510、PDCP層515、RLC層520、MAC層525和PHY層530）。

【0074】 圖6是示出以DL為中心的子訊框的實例的圖600，以DL為中心的子訊框可以用於在無線網路100中進行通訊。以DL為中心的子訊框可以包括控制部分602。控制部分602可以存在於以DL為中心的子訊框的初始或開始部分中。控制部分602可以包括與以DL為中心的子訊框的各個部分相對應的各種排程資訊及/或控制資訊。在一些配置中，如在圖6中所指示的，控制部分602可以是實體DL控制通道（PDCCH）。以DL為中心的子訊框亦可以包括DL資料部分604。DL資料部分604有時可以被稱為以DL為中心的子訊框的有效載荷。DL資料部分604可以包括用於從排程實體（例如，UE或BS）向從屬實體（例如，UE）傳送DL資料的通訊資源。在一些配置中，DL資料部分604可以是實體DL共用通道（PDSCH）。

【0075】 以DL為中心的子訊框亦可以包括公共UL部分606。公共UL部分606有時可以被稱為UL短脈衝、公共UL短脈衝及/或各種其他適當的術語。公共UL部分606可以包括與以DL為中心的子訊框的各個其他部分相對應的回饋資訊。例如，公共UL部分606可以包括與控制部分602相對應的回饋資訊。回饋資訊的非限制性實例可以包括ACK信號、NACK信號、HARQ指示符及/或各種其他適當類型的資訊。公共UL部分606可以包括另外的或替代的資訊，例如，與隨機存取通道（RACH）程序有關的資訊、排程請求（SR）和各種其他適當類型的資

訊。如在圖6中所示出的，DL資料部分604的結束可以與公共UL部分606的開始在時間上是分開的。該時間分隔有時可以被稱為間隙、保護時段、保護間隔及/或各種其他適當的術語。該分隔為從DL通訊（例如，由排程實體（例如，UE）進行的接收操作）到UL通訊（例如，由排程實體（例如，UE）進行的發送）的切換提供了時間。本領域一般技藝人士將理解的是，上文僅僅是以DL為中心的子訊框的一個實例，並且在不必脫離本文所描述的態樣的情況下，可以存在具有相似特徵的替代結構。

【0076】 圖7是示出以UL為中心的子訊框的實例的圖700，以UL為中心的子訊框可以用於在無線網路100中進行通訊。以UL為中心的子訊框可以包括控制部分702。控制部分702可以存在於以UL為中心的子訊框的初始或開始部分中。在圖7中的控制部分702可以類似於上文參考圖6所描述的控制部分。以UL為中心的子訊框亦可以包括UL資料部分704。UL資料部分704有時可以被稱為以UL為中心的子訊框的有效載荷。UL部分可以代表用於從從屬實體（例如，UE）向排程實體（例如，UE或BS）傳送UL資料的通訊資源。在一些配置中，控制部分702可以是實體DL控制通道（PDCCH）。

【0077】 如在圖7中所示出的，控制部分702的結束可以與UL資料部分704的開始在時間上是分開的。該時間分隔有時可以被稱為間隙、保護時段、保護間隔及/或各種其他適當的術語。該分隔為從DL通訊（例如，由排程

實體進行的接收操作）到UL通訊（例如，由排程實體進行的發送）的切換提供了時間。以UL為中心的子訊框亦可以包括公共UL部分706。在圖7中的公共UL部分706可以類似於上文參考圖6所描述的公共UL部分606。公共UL部分706可以另外或替代地包括關於通道品質指示符（CQI）、探測參考信號（SRS）的資訊以及各種其他適當類型的資訊。本領域一般技藝人士將理解的是，上文僅僅是以UL為中心的子訊框的一個實例，以及在不必脫離本文所描述的態樣的情況下，可以存在具有相似特徵的替代結構。

【0078】 在一些情況下，兩個或更多個從屬實體（例如，UE）可以使用側鏈路信號彼此通訊。此種側鏈路通訊的現實應用可以包括公共安全、接近度服務、UE到網路中繼、車輛到車輛（V2V）通訊、萬聯網路（IoE）通訊、IoT通訊、任務關鍵網狀網及/或各種其他適當的應用。通常，側鏈路信號可以代表從一個從屬實體（例如，UE 1）向另一個從屬實體（例如，UE 2）傳送的信號，而無需經由排程實體（例如，UE或BS）來中繼該通訊，即使排程實體可以用於排程及/或控制目的。在一些實例中，可以使用經許可頻譜來傳送側鏈路信號（不同於通常使用非許可頻譜的無線區域網路）。

【0079】 UE可以在各種無線電資源配置中操作，該等配置包括與使用專用資源集合（例如，無線電資源控制（RRC）專用狀態等）來發送引導頻相關聯的配置，或

與使用公共資源集合（例如，RRC公共狀態等）來發送引導頻相關聯的配置。當在RRC專用狀態下操作時，UE可以選擇專用資源集合來向網路發送引導頻信號。當在RRC公共狀態下操作時，UE可以選擇公共資源集合來向網路發送引導頻信號。在任一種情況下，由UE發送的引導頻信號可以由諸如AN或DU或其部分之類的一或多個網路存取設備來接收。每個進行接收的網路存取設備可以被配置為接收和量測在公共資源集合上發送的引導頻信號，並且亦接收和量測在被分配給UE的專用資源集合上發送的引導頻信號，其中該網路存取設備是針對該等UE進行監測的網路存取設備集合中的針對該UE的成員。進行接收的網路存取設備或者進行接收的網路存取設備向其發送對引導頻信號的量測的CU中的一者或多者可以使用量測來辨識針對UE的服務細胞，或者發起對針對UE中的一或多個UE的服務細胞的改變。

在金鑰產生中對網路策略的示例性合併

【0080】 如前述，正在為5G引入新的空中介面，其包括如下的特徵：該等特徵包括以寬頻寬（例如，80 MHz以上）為目標的增強型行動寬頻（eMBB）、以高載波頻率（例如，60 GHz）為目標的毫米波（mmW）、以非向後相容MTC技術為目標的大容量MTC（mMTC）、以及以超可靠低延時通訊（URLLC）為目標的任務關鍵。

【0081】 隨著針對5G的服務和技術持續進化，5G能夠支援各種不同的部署場景。例如，在當前的5G架構中，

在網路中負責執行不同功能的一或多個網路節點（例如，安全錨功能單元（SEAF）、存取和行動性管理功能單元（AMF）、通信期管理功能單元（SMF）等）可以是共置的或者是在實體上分離的。

【0082】 在5G中引入SEAF以將安全錨保持在實體上安全的位置上，即使需要將AMF移動及/或定位到靠近網路邊緣（例如，RAN）。因此，在一些部署中，SEAF可以與AMF共置，而在其他部署中，SEAF可以與AMF分離（例如，SEAF和AMF可以各自具有獨立的功能）。類似地，SMF可以與AMF和SEAF分離。在一些情況下，SMF可以與AMF在實體上分離，並且可以在與AMF不同的安全域內（例如，在網路共用場景的情況下）。在一些情況下，SMF可以是特定於切片的。

【0083】 圖8圖示根據本案內容的某些態樣的5G架構800的參考實例，在5G架構800中，一或多個網路節點可以是在實體上分離的。具體而言，架構800圖示如下的部署場景的參考實例：在該部署場景中，SEAF與AMF是在實體上分離的（例如，與在其他部署場景中的共置的SEAF/AMF相反）。

【0084】 如所示出的，5G架構800可以包括多個切片。每個切片可以支援不同的服務，例如，萬聯網路（IoE）、URLLC、eMBB、車輛通訊（亦即，諸如車輛到車輛（V2V）、車輛到基礎設施（V2I）、車輛到行人（V2P）、車輛到網路（V2N）等的V2X）。

【0085】 切片可以被定義為完整的邏輯網路，其包括網路功能的集合以及用於提供某些網路能力和網路特性所必需的相應資源，該邏輯網路可以包括5G-AN和5G-CN兩者。更具體而言，切片可以是被附隨在一起以滿足特定用例或商業模型的要求的充分配置的網路功能、網路應用和底層雲基礎設施的組成。在一些情況下，不同的切片可以被指派不相交的資源，並且可以具有不同的要求（例如延時及/或功率）。

【0086】 在該實例中，AMF可以被配置為同時服務多個切片。例如，AMF可以在UE與網路切片之間提供行動性管理NAS安全錨。SMF通常被配置為執行服務授權/認證以支援特定於服務（切片）的PDU通信期建立。SMF亦可以執行如下功能，例如修改和釋放在使用者平面功能單元（UPF）與RAN之間維護的隧道。使用者平面安全可以在UDF處終止。在一些情況下，SMF能夠支援特定於服務的QoS。

【0087】 圖9圖示根據本案內容的某些態樣的5G架構900的另一參考實例，在5G架構900中，一或多個網路節點（例如，SEAF、AMF、SMF等）可以是在實體上分離的。在一些情況下，5G安全架構可以被設計為在本端利用協力廠商認證伺服器功能單元（AUSF）（例如，協力廠商AAA）來支援針對PDU通信期授權的二次認證。服務認證賦能特定於服務的PDU通信期的建立。與圖8相似，使用者平面安全可以在UPF處終止，並且可以

支援特定於服務的QoS。SMF能夠直接地對接到協力廠商AAA或經由SEAF與協力廠商AAA進行互動。

【0088】 如所指出的，由於5G網路可能持續進化，因此可能希望向UE提供關於特定的網路配置、能力、安全資訊等的資訊（本文統稱為網路策略資訊）。然而，在當前架構中，由於在UE與服務網路之間的唯一控制平面介面是N1（其用於在UE與AMF之間的NAS連接），所以不可能利用當前技術來以安全的方式向UE提供網路策略資訊。

【0089】 例如，參考架構800，由於AMF可能是具有與UE的信號傳遞連接（例如，基於NAS信號傳遞）的唯一實體，所以AMF可能會錯誤地向UE通知關於從另一網路節點（例如，SEAF、SMF等）接收的任何網路安全性原則資訊。因此，若網路策略資訊包括關於AMF和SEAF是分離的資訊，則當前技術可能無法安全地向UE通知AMF和SEAF是分離的，此是因為UE可能僅具有與AMF的信號傳遞連接（例如，與亦具有與SEAF的信號傳遞連接的情況相反）。

【0090】 在此種情況下，獨立（欺詐）AMF可能會聲稱其是與SEAF共置的，此是UE無法偵測到的場景。此種獨立AMF（欺詐）可能會修改網路安全能力、通信期管理NAS保護、特定於切片的安全能力/要求等，以危害在UE與網路之間的連接/通信期。

【0091】 此外，在沒有準確的（安全的）網路策略資訊的情況下，UE可能遭受（例如，對PDU通信期建立的）打壓（bidding down）攻擊。在打壓場景的一個實例中，AMF可以處於與SMF不同的安全域中。例如，在一種情況下，AMF可以在服務網路中位於UE（或RAN）附近（例如，其可能是較不安全的位置），而SMF可以位於網路的深處。在一種情況下，AMF可以處於服務網路（例如，VPLMN）中，而SMF處於歸屬網路中。

【0092】 然而，儘管AMF可以在與SMF不同的安全域中，但是SMF仍然可以負責授權特定於切片的PDU通信期建立（例如，基於無法由AMF存取的特定於切片的訂製資訊）。例如，SMF通常是與AMF在邏輯上分離的網路功能單元，並且負責PDU通信期授權和管理。如前述，SMF可以是特定於切片的，並且因此可以與UE交換特定於切片的PDU通信期參數。

【0093】 然而，由UE所請求的並且由SMF所配置的PDU通信期參數（諸如經授權的QoS規則、SSC模式、S-NSSAI、所分配的IPv4位址等）不應當由在UE與SMF之間的中間節點（例如，包括AMF）修改。更確切而言，此種參數應當由SMF使用從SEAF獲得的特定金鑰來保護，並且在UE處可經由推導出相同的SMF金鑰來驗證。因此，在AMF與SEAF分離的情況下，（惡意的或被盜用的）AMF可能修改由UE所請求的或由SMF所

授權的通信期資訊，例如以使安全性、QoS或其他封包處理降級。

【0094】 因此，本文所提出的各態樣提供了用於安全地向UE通知網路策略資訊例如以最小化打壓攻擊的技術。具體而言，各態樣提供了用於將網路策略資訊合併到用於保護在UE與AMF之間的NAS連接的金鑰（例如，K_{AMF}）推導中的技術。如下文所描述的，經由將網路策略資訊合併到金鑰推導中，UE能夠偵測從AMF所接收的任何網路策略資訊是否已被改變/修改/盜用。

【0095】 注意的是，儘管本文所描述的技術可以用於防範對PDU通信期建立的打壓攻擊，但是本文提出的各態樣亦可以用於防範由在SEAF與UE之間的節點進行的UE策略打壓。亦即，如下文所描述的，本文所提出的各態樣亦可以用於例如經由將UE策略資訊（例如，UE安全特徵及/或UE能力（包括網路能力、安全能力或其任何組合））合併到金鑰（例如，K_{AMF}）推導中來保護UE策略資訊。可以在註冊/附著請求訊息中向網路提供UE策略資訊。

【0096】 根據某些態樣，K_{AMF}推導可以用於保護在網路中交換的參數。具體而言，當UE向網路註冊時，SEAF可以經由以下操作來向UE通知（例如，由UE所接收的）網路（安全）策略資訊（例如，網路配置、能力、安全特徵等）及/或UE策略資訊：在金鑰（例如，K_{AMF}）推導中合併網路策略資訊及/或UE策略資訊。

【0097】 例如，SEAF可以基於網路策略資訊、UE策略資訊、新鮮度參數或其任何組合來推導出AMF金鑰(例如，K_{AMF})，並且將該金鑰發送給AMF，使得AMF和UE可以建立NAS安全上下文，並且SEAF亦可以向UE通知從UE所接收的UE策略資訊。AMF和UE可以從K_{AMF}推導出加密和完整性保護金鑰並且(例如，在N1介面上)保護NAS訊息。

【0098】 經由將網路策略資訊合併到K_{AMF}推導中，可以防止AMF執行未授權的行為(諸如經由修改從SEAF接收的網路策略資訊來打壓網路特徵)，此是因為在網路策略資訊中的改變導致在UE處的不同K_{AMF}推導。類似地，經由將UE策略資訊合併到K_{AMF}推導中，可以防止在UE與SEAF之間的網路節點經由修改UE能力來打壓UE能力，此是因為在UE能力中的改變亦將導致不同的K_{AMF}推導。

【0099】 圖10圖示用於無線通訊的示例性操作1000。根據某些態樣，操作1000可以例如由使用者設備來執行以用於與網路建立安全(例如，NAS)連接。

【0100】 操作1000可以開始於1002處，其中UE(例如，從AMF)接收用於與網路建立安全連接的第一訊息(例如，安全模式命令(SMC)訊息)。第一訊息包括網路策略資訊(例如，網路配置、能力、安全特徵等)。在1004處，UE部分地基於網路策略資訊來產生第一金鑰(例如，K_{AMF})。

【0101】 在一些態樣中，網路策略資訊包括關於當與網路建立通訊通信期時UE是否將從網路中的SMF接收通信期管理符記的指示。在一些態樣中，網路策略資訊包括關於AMF是否在網路中與SEAF共置的指示。在一些態樣中，網路策略資訊包括AMF的安全級別。在一些態樣中，網路策略資訊包括SEAF的安全域、AMF的安全域或其任何組合。在一些態樣中，可能已經回應於從UE發送給網路的UE策略資訊而形成了網路策略資訊。在一些態樣中，第一金鑰可以是基於被發送給網路的UE策略資訊來決定的。

【0102】 在1006處，UE使用第一金鑰來驗證網路策略資訊是有效的。例如，在一些情況下，UE可以部分地基於第一金鑰來決定第一訊息（包含網路策略資訊）是否是有效的。

【0103】 如下文更詳細描述的，在一些情況下，第一訊息可以是SMC訊息，該SMC訊息是利用基於第二金鑰（例如，從SEAF提供給AMF的K_{AMF}）推導出的保護金鑰來進行完整性保護的。UE可以經由基於第一金鑰來執行對第一訊息的完整性驗證來決定第一訊息（及/或在其中包含的網路策略資訊）是否是有效的。在一個態樣中，若對第一訊息的完整性驗證是正確的，則UE可以決定第一訊息是有效的。

【0104】 若UE決定第一金鑰與第二金鑰相同，則UE可以決定對第一訊息的完整性驗證是正確的。UE可以基

於決定第一金鑰與第二金鑰是相同的來決定網路策略資訊是有效的。同樣地，若對第一訊息的完整性驗證是不正確的，則UE可以決定第一訊息是無效的。若第一金鑰不同於第二金鑰，則UE可以決定對第一訊息的完整性驗證是不正確的。UE可以基於決定第一金鑰與第二金鑰是不同的來決定網路策略資訊是無效的。

【0105】 圖11圖示用於無線通訊的示例性操作1100。根據某些態樣，操作1100可以例如由網路節點(例如，SEAF）來執行以用於向UE安全地提供網路策略資訊。

【0106】 操作1100可以開始於1102處，其中網路節點至少部分地基於網路策略資訊來產生用於另一網路節點（例如，AMF）的金鑰（例如，K_{AMF}）。如所指出的，網路策略資訊可以包括關於另一網路節點（例如，AMF）是否與該網路節點共置的指示。在一些情況下，網路策略資訊可以包括以下各項中的至少一項：網路節點的安全級別，或者關於網路中的SMF是否要產生用於UE與網路之間的通訊通信期的SM符記並且將SM符記發送給UE的指示。該金鑰用於在UE與網路節點之間建立安全連接。

【0107】 在一些態樣中，網路節點可以接收包括UE策略（或能力）資訊的註冊訊息/附著請求訊息。網路節點可以將所接收的UE策略資訊合併到針對另一網路節點的金鑰（例如，K_{AMF}）推導中。例如，在圖11的1102處，網路節點可以部分地基於網路策略資訊、新鮮度參數、

UE策略資訊或其任何組合來產生用於另一網路節點（例如，AMF）的金鑰（例如，K_{AMF}）。

【0108】 在1104處，網路節點將金鑰發送給另一網路節點。在一些態樣中，網路節點亦可以向網路節點發送以下各項中的至少一項：網路策略資訊或者網路策略資訊有效的時間量。

【0109】 圖12是圖示根據本案內容的某些態樣的示例性註冊程序的撥叫流程圖，該註冊程序允許SEAF（例如，經由在金鑰推導中合併策略資訊及/或UE策略資訊）安全地向UE通知網路（安全）策略資訊及/或UE策略資訊。

【0110】 在一些態樣中，如所示出的，UE可以初始地向網路（例如，AMF、SEAF等）發送註冊請求/附著請求。註冊請求/附著請求包括UE策略（能力）。隨後，在步驟1處，UE執行與網路的認證/註冊程序。UE和SEAF可以基於新的認證或基於先前的認證來建立共用錨金鑰（K_{SEAF}）。在註冊期間，AMF可以從SEAF請求金鑰（K_{AMF}）。

【0111】 在步驟2處，SEAF針對AMF產生（例如，推導出）用於將UE註冊到網路的K_{AMF}。K_{AMF}推導將網路策略資訊（例如，網路配置、能力、安全特徵等）及/或UE策略資訊合併。在一個態樣中，網路策略資訊可以包括AMF類型，例如，共置AMF/SEAF、獨立AMF等。

【0112】 例如，網路策略資訊可以包括一或多個SEAF/AMF分離位元。若請求K_{AMF}的AMF是與SEAF分離的獨立AMF，則SEAF可以將SEAF/AMF分離位元設置為第一值（例如，1）。若請求K_{AMF}的AMF是共置AMF/SEAF，則SEAF可以將SEAF/AMF分離位元設置為不同的第二值（例如，0）。在一個態樣中，K_{AMF}推導亦可以合併用於防止重放攻擊的一或多個新鮮度參數。此種新鮮度參數的實例可以包括（在UE和SEAF兩者處維護的）計數器、在UE與SEAF之間交換的隨機值，或其任何組合。在一個態樣中，SEAF可以使用以下等式（1）來產生（推導出）K_{AMF}：

K_{AMF} = KDF(K_{SEAF}，新鮮度參數，網路策略資訊，UE策略）　　（1）

其中KDF是金鑰推導函數（例如，HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-512、PRF-X（其輸出大小為X的假性隨機函數）），K_{SEAF}是服務網路中的錨保護金鑰（並且保存在SEAF處），新鮮度參數是用於防止重放攻擊的計數器、隨機值，網路策略資訊包括網路配置、能力、安全特徵等，以及 UE策略包括UE能力資訊及/或UE安全資訊中的至少一項。

【0113】 在步驟3處，SEAF向AMF提供K_{AMF}、新鮮度參數和網路策略資訊。在一些態樣中，SEAF亦可以在步驟3處向AMF提供（例如，重複）UE策略。在步驟4處，AMF向UE發送NAS安全模式命令（SMC）。在一

些態樣中，AMF亦可以在步驟4處向UE提供（例如，重複）UE策略。NAS SMC可以包括從SEAF獲得的新鮮度參數和網路策略資訊，並且可以基於K_{AMF}來對NAS SMC進行完整性保護。例如，在從SEAF接收K_{AMF}時，AMF可以基於K_AMF來推導出NAS完整性保護金鑰（例如，K_{NASINT}），並且使用KNASINT來對NAS SMC訊息進行完整性保護。

【0114】 在步驟5處，UE使用K_{SEAF}和NAS SMC訊息中的資訊（例如，新鮮度參數、網路策略資訊等）來產生（例如，推導出）K_{AMF}，並且驗證NAS SMC訊息。亦即，UE可以偵測是否已經存在（例如，由AMF）對網路策略資訊的任何改變，此是因為在網路策略資訊中的任何改變將導致在UE處不同的K_{AMF}推導。當UE經由將由UE產生的K_{AMF}與使用K_{AMF}對NAS SMC的完整性保護進行比較來檢查對使用的NAS SMC的完整性保護時，UE可以偵測到此種變化。因此，決定對SMC的完整性驗證是正確的，此意味著由UE產生的K_{AMF}和（從SEAF）提供給AMF的K_{AMF}是相同的，此進而意味著（從AMF）提供給UE的網路策略資訊是有效的。

【0115】 假設對SMC的驗證是正確的，UE（在步驟6處）向AMF發送NAS安全模式完成訊息。在一些態樣中，UE亦可以偵測（被提供給網路的）UE策略資訊是否已被任何中間網路節點修改。亦即，在一些態樣中，UE可以基於UE策略資訊（例如，除了網路策略資訊之外或

作為網路策略資訊的替代）來產生K_{AMF}，以（例如，基於由UE產生的K_{AMF}和（從SEAF）提供給AMF的K_{AMF}是否是相同的）決定UE策略資訊是否已被修改。

【0116】 注意的是，儘管圖12中的撥叫流程描述了將網路策略資訊合併到金鑰推導中以便安全地向UE通知網路策略資訊，本文所提出的技術亦可以用於保護UE安全特徵。亦即，除了網路策略資訊之外或作為網路策略資訊的替代，金鑰（K_{AMF}）推導可以合併UE能力（包括UE安全特徵），其中UE能力是在註冊/附著請求訊息中提供給網路的。

【0117】 在圖10-圖12中所描述的技術可以用於經由限制金鑰推導中的金鑰使用來防止AMF修改其中繼給UE的任何網路能力參數。然而，儘管該等技術可能對於防止對網路能力的打壓是有用的，但是此種技術可能不足以防止PDU通信期參數打壓（例如，SM NAS符記）。

【0118】 因此，本文所提出的各態樣提供了可以用於防止（例如，對PDU通信期建立及/或網路能力參數的）打壓攻擊的技術。

【0119】 更具體而言，當UE註冊到網路時，SEAF向AMF提供網路策略資訊（例如，網路配置、（安全）能力等）和經完整性保護的網路策略資訊（例如，網路策略符記）連同K_{AMF}。網路策略資訊是使用K_{SEAF}來進行完整性保護的。網路策略符記搭載在NAS安全模式命令上

並且被提供給UE。網路策略符記防止位於SEAF與UE之間的任何網路功能單元修改網路能力。

【0120】 圖13圖示用於無線通訊的示例性操作1300。根據某些態樣，操作1300可以例如由使用者設備來執行，以用於與網路建立安全（例如，NAS）連接。

【0121】 操作1300可以開始於1302處，其中UE基於與網路的認證程序來建立UE與網路中的SEAF之間共享的錨金鑰（例如，K_{SEAF}）。在1304處，UE接收用於與網路建立安全連接的第一訊息（例如，SMC訊息）。第一訊息包括用於與網路的通訊通信期的網路策略符記、網路策略資訊、網路策略資訊有效的第一時間量以及用於安全連接的第一金鑰有效的第二時間量。網路策略符記包括與網路策略資訊相關聯的完整性保護資訊。

【0122】 在1306處，在與網路建立安全連接之前，UE基於從所共享的錨金鑰、網路策略資訊、第一時間量和第二時間量推導出的金鑰來決定網路策略符記是否是有效的。在一些態樣中，決定網路策略符記是否是有效的包括：基於從所共享的錨金鑰推導出的金鑰來驗證完整性保護資訊。在一些態樣中，UE可以向網路發送UE策略資訊（例如，UE能力資訊、UE安全資訊等）。UE可以基於被發送給網路的UE策略資訊來產生金鑰。在一些情況下，網路策略資訊可以是基於UE策略資訊的。

【0123】 圖14圖示用於無線通訊的示例性操作1400。根據某些態樣，操作1400可以例如由網路節點（例

如，SEAF）來執行，以用於向UE安全地提供網路策略資訊。

【0124】 操作1400可以開始於1402處，其中網路節點基於與UE的認證程序來建立在網路中網路節點與UE之間共享的錨金鑰（例如，K_{SEAF}）。在1404處，網路節點部分地基於錨金鑰、網路策略資訊和網路策略符記有效的第一時間量來產生網路策略符記（例如，K_{token}）。網路策略符記包括與網路策略資訊相關聯的完整性保護資訊。在1406處，網路節點產生用於另一網路節點（例如，AMF）的金鑰（例如，K_{AMF}）。在1408處，網路節點將金鑰、網路策略資訊和網路策略符記發送給另一網路節點。

【0125】 在一些態樣中，如上文所描述的，網路節點可以將UE策略資訊合併到金鑰（例如，K_{AMF}）推導中，例如以防止中間節點修改從UE接收的UE策略資訊。如所指出的，網路節點可以經由註冊/附著請求訊息來接收UE策略資訊。

【0126】 圖15是圖示根據本案內容的某些態樣的允許SEAF防止對PDU通信期建立的打壓攻擊的示例性註冊程序的撥叫流程圖。

【0127】 如所示出的，在步驟1處，UE執行與網路的註冊程序。UE和SEAF可以基於新的認證或基於先前的認證來建立共用錨金鑰（K_{SEAF}）。在註冊期間，AMF可以從SEAF請求金鑰（K_{AMF}）。儘管未圖示，但是在

一些情況下，UE可以經由註冊/附著請求訊息向網路提供UE策略資訊（例如，UE能力資訊、UE安全資訊等）。

【0128】 在步驟2處，SEAF針對AMF產生用於將UE註冊到網路的K_{AMF}。SEAF可以使用K_{SEAF}和一或多個第一新鮮度參數來產生K_{AMF}。另外，SEAF使用K_{SEAF}、一或多個第二新鮮度參數（例如，以防止重放攻擊）和網路策略資訊來產生網路策略符記。如所指出的，網路策略符記是網路策略資訊的訊息認證碼（或完整性保護資訊）。與圖12類似，網路策略資訊可以包括一或多個SEAF/AMF分離位元。在一些態樣中，SEAF可以進一步基於UE策略資訊來產生K_{AMF}。

【0129】 在步驟3處，SEAF向AMF提供K_{AMF}、第一和第二新鮮度參數、網路策略符記和網路策略資訊。在步驟4處，AMF向UE發送NAS安全模式命令。NAS安全模式命令包括從SEAF獲得的網路策略資訊、第一和第二新鮮度參數以及網路策略符記。

【0130】 在步驟5處，UE使用K_{SEAF}來對網路策略符記執行驗證程序。若驗證是成功的，則UE使用K_{SEAF}來推導出K_{AMF}，並且使用所推導出的K_{AMF}對NAS安全模式命令執行驗證程序。假設驗證了NAS安全模式命令，UE（在步驟6處）向AMF發送NAS安全模式完成訊息。以此種方式，SEAF可以以安全的方式直接地向UE指示網路能力（此是因為符記是基於UE與SEAF之間的金鑰來產生和驗證的）。

【0131】 注意的是，在一些態樣中，（與在圖12中的SEAF相比較而言）（用於圖15的）SEAF可能必須針對網路策略產生來維護UE的額外狀態（例如，新鮮度參數），以防止重放攻擊。此可以類似於在UE與SEAF之間維持連接狀態、可能傾向於不同步的連接。此外，注意的是，與在圖13-圖15中所描述的技術相似的技術亦可以用於防範對UE策略資訊（包括UE安全資訊及/或UE能力資訊）的打壓攻擊。

【0132】 本文所揭示的方法包括用於實現所描述的方法的一或多個步驟或動作。方法步驟及/或動作可以在不脫離請求項的範圍的情況下彼此互換。換言之，除非指定了步驟或動作的特定的順序，否則在不脫離請求項的範圍的情況下，可以修改特定步驟及/或動作的順序及/或對特定步驟及/或動作的使用。

【0133】 如本文所使用的，提及項目列表「中的至少一個」的短語指的是彼等項目的任何組合，包括單個成員。作為實例，「a、b或c中的至少一個」意在涵蓋a、b、c、a-b、a-c、b-c和a-b-c、以及與相同元素的倍數（例如，a-a、a-a-a、a-a-b、a-a-c、a-b-b、a-c-c、b-b、b-b-b、b-b-c、c-c和c-c-c或a、b和c的任何其他排序）的任何組合。

【0134】 如本文所使用的，術語「決定」包含各種各樣的動作。例如，「決定」可以包括計算、運算、處理、推導、調查、檢視（例如，在表、資料庫或另一資料結構中

檢視）、查明等。此外，「決定」可以包括接收（例如，接收資訊）、存取（例如，存取記憶體中的資料）等。此外，「決定」可以包括解決、選擇、挑選、建立等。

【0135】 在一些情況下，設備可以具有用於輸出訊框以進行傳輸的介面，而不是實際發送訊框。例如，處理器可以經由匯流排介面將訊框輸出給用於傳輸的RF前端。類似地，設備可以具有用於獲得從另一設備接收的訊框的介面，而不是實際接收訊框。例如，處理器可以經由匯流排介面從用於傳輸的RF前端獲得（或者接收）訊框。

【0136】 上文描述的方法的各種操作可以由能夠執行相應的功能的任何適當的手段來執行。該手段可以包括各種硬體及/或軟體部件及/或模組，包括但不限於電路、特殊應用積體電路（ASIC）或處理器。通常，在存在圖中所示出的操作的情況下，彼等操作可以具有相應的具有相似編號的配對手段加功能部件。

【0137】 例如，用於發送的手段、用於接收的手段、用於決定的手段、用於執行的手段、用於參與的手段、用於指示的手段、用於建立的手段、用於驗證的手段、用於發送的手段、用於通訊的手段、用於儲存的手段、用於進入的手段、用於保護的手段、用於防止的手段、用於退出的手段、用於產生的手段、用於轉發的手段及/或用於提供的手段可以包括BS 110或UE 120處的一或多個處理器或天線，例如，在BS 110處的發送處理器420、控制器/處理器440、接收處理器438或天線434，及/或在UE

120處的發送處理器464、控制器/處理器480、接收處理器458或天線452。

【0138】結合本案內容描述的各種說明性的邏輯區塊、模組和電路可以利用被設計為執行本文所描述的功能的通用處理器、數位信號處理器（DSP）、特殊應用積體電路（ASIC）、現場可程式設計門控陣列（FPGA）或其他可程式設計邏輯裝置（PLD）、個別閘門或電晶體邏輯、個別硬體部件或其任何組合來實現或執行。通用處理器可以是微處理器，但是在替代的方案中，處理器可以是任何商業上可獲得的處理器、控制器、微控制器或狀態機。處理器亦可以被實現為計算設備的組合，例如，DSP和微處理器的組合、多個微處理器、與DSP核相結合的一或多個微處理器，或任何其他此種配置。

【0139】若用硬體來實現，則示例性硬體設定可以包括無線節點中的處理系統。處理系統可以是利用匯流排架構來實現的。根據處理系統的具體應用和整體設計約束，匯流排可以包括任意數量的互連匯流排和橋接器。匯流排可以將包括處理器、機器可讀取媒體和匯流排介面的各種電路連接在一起。除此以外，匯流排介面亦可以用於經由匯流排將網路介面卡連接到處理系統。網路介面卡可以用於實現PHY層的信號處理功能。在使用者終端120（參見圖1）的情況下，使用者介面（例如，小型鍵盤、顯示器、滑鼠、操縱桿等）亦可以連接到匯流排。匯流排亦可以連接各種其他電路，例如，定時源、周邊設備、電壓調節器、

功率管理電路等，該等電路在本領域中是公知的，並且因此，將不再進行描述。處理器可以是利用一或多個通用及/或專用處理器來實現的。實例係包括微處理器、微控制器、DSP處理器和可以執行軟體的其他電路。本領域技藝人士將認識到如何根據特定應用和對整個系統施加的整體設計約束來最佳地實現針對處理系統所描述的功能。

【0140】 若用軟體來實現，則功能可以是作為在電腦可讀取媒體上的一或多個指令或代碼來儲存或發送的。軟體應廣義地解釋為意指指令、資料或其任何組合，無論其是被稱為軟體、韌體、中介軟體、微代碼、硬體描述語言還是其他術語。電腦可讀取媒體包括電腦儲存媒體和通訊媒體兩者，該通訊媒體包括促進將電腦程式從一個地方轉移到另一個地方的任何媒體。處理器可以負責管理匯流排和一般處理，包括對儲存在機器可讀儲存媒體上的軟體模組的執行。電腦可讀取儲存媒體可以耦合到處理器，使得處理器可以從儲存媒體讀取資訊，以及將資訊寫入儲存媒體。在替代方案中，儲存媒體可以是處理器的組成部分。舉例而言，機器可讀取媒體可以包括傳輸線、經由資料調變的載波及/或與無線節點分開的在其上儲存有指令的電腦可讀取儲存媒體，所有該等皆可以由處理器經由匯流排介面來存取。替代地或者另外，機器可讀取媒體或其任何部分可以整合到處理器中，諸如該情況可以是快取記憶體及/或通用暫存器檔。舉例而言，機器可讀儲存媒體的實例可以包括RAM(隨機存取記憶體)、快閃記憶體、ROM

（唯讀記憶體）、PROM（可程式設計唯讀記憶體）、EPROM（可抹除可程式設計唯讀記憶體）、EEPROM（電子可抹除可程式設計唯讀記憶體）、暫存器、磁碟、光碟、硬碟，或任何其他適當的儲存媒體，或其任何組合。機器可讀取媒體可以體現在電腦程式產品中。

【0141】 軟體模組可以包括單個指令或多個指令，並且可以分佈在數個不同的程式碼片段上，分佈在不同程式之中以及跨越多個儲存媒體來分佈。電腦可讀取媒體可以包括多個軟體模組。軟體模組包括指令，該等指令當由諸如處理器之類的裝置執行時使得處理系統執行各種功能。軟體模組可以包括發送模組和接收模組。每個軟體模組可以位於單個儲存裝置中，或者是跨越多個儲存裝置來分佈的。舉例而言，當發生觸發事件時，可以將軟體模組從硬碟載入到RAM中。在對軟體模組的執行期間，處理器可以將指令中的一些指令載入到快取記憶體中，以提高存取速度。隨後，可以將一或多個快取記憶體行載入到通用暫存器檔中，以用於由處理器來執行。當提及下文的軟體模組的功能時，將理解的是，此種功能是由處理器在執行來自該軟體模組的指令時實現的。

【0142】 此外，將任何連接適當地稱為電腦可讀取媒體。例如，若使用同軸電纜、光纖光纜、雙絞線、數位使用者線路（DSL）或諸如紅外線（IR）、無線電和微波之類的無線技術，從網站、伺服器或其他遠端源反射軟體，則同軸電纜、光纖光纜、雙絞線、DSL或諸如紅外

線、無線電和微波之類的無線技術被包括在媒體的定義中。如本文所使用的，磁碟和光碟包括壓縮光碟（CD）、雷射光碟、光碟、數位多功能光碟（DVD）、軟碟和藍光®光碟，其中磁碟通常磁性地複製資料，而光碟則利用雷射來光學地複製資料。因此，在一些態樣中，電腦可讀取媒體可以包括非暫時性電腦可讀取媒體（例如，有形媒體）。此外，對於其他態樣，電腦可讀取媒體可以包括暫時性電腦可讀取媒體（例如，信號）。上述的組合亦應當被包括在電腦可讀取媒體的範圍內。

【0143】 進一步地，應當明白的是，若適用的話，用於執行本文所描述的方法和技術的模組及/或其他適當的手段可以由使用者終端及/或基地台下載及/或以其他方式獲得。例如，此種設備可以耦合到伺服器，以促進對用於執行本文所描述的方法的手段的傳送。替代地，本文所描述的各種方法可以是經由儲存手段（例如，RAM、ROM、諸如壓縮光碟（CD）或軟碟等的實體儲存媒體等）來提供的，使得使用者終端及/或基地台可以在與該設備耦合或向該設備提供儲存手段時獲得各種方法。此外，可以利用用於向設備提供本文中所描述的方法和技術的任何其他適當的技術。

【0144】 要理解的是，請求項不限於上文示出的精確配置和部件。在不脫離請求項的範疇的情況下，可以對上文描述的方法和裝置的佈置、操作和細節進行各種修改、改變和變型。

【符號說明】

【0145】

100 無線網路

102a 巨集細胞

102b 巨集細胞

102c 巨集細胞

102x 微微細胞

102y 毫微微細胞

102z 毫微微細胞

110 基地台

110a 基地台

110b 基地台

110c 基地台

110r 中繼站

110x 基地台

110y 基地台

110z 基地台

120 使用者設備

120r 使用者設備

120x 使用者設備

120y 使用者設備

130 網路控制器

200 無線電存取網路（RAN）

202 存取節點控制器（ANC）

204 下一代核心網路（NG-CN）

206 5G存取節點

208 TRP

210 下一代AN（NG-AN）

300 分散式RAN

302 集中式核心網路單元（C-CU）

304 集中式RAN單元（C-RU）

306 DU

412 資料來源

420 發送處理器

430 發送（TX）多輸入多輸出（MIMO）處理器

432a 調變器（MOD）

432t 調變器（MOD）

434a 天線

434t 天線

436 MIMO偵測器

438 接收處理器

439 資料槽

440 控制器/處理器

442 記憶體

444 排程器

452a 天線

452r 天線

454a 解調器（DEMOD）

454r 解調器（DEMOD）

456 MIMO偵測器

458 接收處理器

460 資料槽

462 資料來源

464 發送處理器

466 TX MIMO處理器

480 控制器/處理器

482 記憶體

500 圖

505-a 第一選項

505-b 第二選項

510 無線電資源控制（RRC）層

515 封包資料彙聚協定（PDCP）層

520 無線電鏈路控制（RLC）層

525 媒體存取控制（MAC）層

530 實體（PHY）層

600 圖

602 控制部分

604 DL資料部分

606 公共UL部分

700 圖

702 控制部分

704 UL資料部分

706 公共UL部分

800 5G架構

900 5G架構

1000 操作

1002 步驟

1004 步驟

1006 步驟

1100 操作

1102 步驟

1104 步驟

1300 操作

1302 步驟

1304 步驟

1306 步驟

1400 操作

1402 步驟

1404 步驟

1406 步驟

1408 步驟

【生物材料寄存】

【0146】 國內寄存資訊 (請依寄存機構、日期、號碼順序註記)

無

【0147】 國外寄存資訊 (請依寄存國家、機構、日期、號碼順序註記)

無

【發明申請專利範圍】

【第1項】 一種用於由一使用者設備（UE）進行無線通訊的方法，包括以下步驟：

接收用於與一網路建立一安全連接的一第一訊息，其中該第一訊息包括網路策略資訊；

藉由一金鑰推導函數（KDF）來產生一第一金鑰，其中該網路策略資訊是導入該KDF的一輸入；及

至少部分地基於該第一金鑰來驗證該網路策略資訊。

【第2項】 根據請求項1之方法，其中驗證該網路策略資訊包括以下步驟：部分地基於該第一金鑰來決定該第一訊息是否是有效的。

【第3項】 根據請求項2之方法，其中：

該第一訊息是利用從一第二金鑰推導出的一保護金鑰來進行完整性保護的；及

決定該第一訊息是否是有效的包括：基於該第一金鑰來執行對該第一訊息的完整性驗證。

【第4項】 根據請求項2之方法，亦包括以下步驟：

若該決定是該第一訊息是有效的，則與該網路建立一安全連接。

【第5項】 根據請求項1之方法，其中該第一訊息亦包括該網路策略資訊有效的一時間量。

【第6項】 根據請求項5之方法，其中該第一金鑰是進一步基於以下各項中的至少一項來產生的：該UE與該網路中的一安全錨功能單元（SEAF）之間共享的一錨金鑰，或者該網路策略資訊有效的該時間量。

【第7項】 根據請求項6之方法，亦包括以下步驟：在接收該第一訊息之前執行與該SEAF的一認證程序或註冊程序中的至少一項，其中該錨金鑰是基於該認證程序或註冊程序中的至少一項來建立的。

【第8項】 根據請求項1之方法，其中該網路策略資訊包括關於當與該網路建立一通訊通信期時該UE是否將從該網路中的一通信期管理功能單元（SMF）接收一通信期管理符記的一指示。

【第9項】 根據請求項1之方法，其中該第一訊息是從該網路中的一存取和行動性管理功能單元（AMF）接收的。

【第10項】 根據請求項9之方法，其中該網路策略資訊包括關於該AMF是否與該網路中的一安全錨功能單元（SEAF）共置的一指示。

【第11項】 根據請求項9之方法，其中該網路策略資訊包括該AMF的一安全級別。

【第12項】 根據請求項1之方法，其中：

該第一訊息是從該網路中的一存取和行動性管理功

能單元（AMF）接收的；及

建立該安全連接包括：向該AMF發送一第二訊息。

【第13項】 根據請求項12之方法，其中：

該第一訊息是一安全模式命令（SMC）訊息；及

該第二訊息是一SMC完成訊息。

【第14項】 根據請求項12之方法，其中該安全連接包括一非存取層（NAS）安全連接。

【第15項】 根據請求項1之方法，亦包括以下步驟：

向該網路發送UE策略資訊，其中該UE策略資訊包括以下各項中的至少一項：UE能力資訊，或者UE安全資訊。

【第16項】 根據請求項15之方法，其中產生該第一金鑰是基於被發送給該網路的該UE策略資訊的。

【第17項】 根據請求項15之方法，其中該網路策略資訊是基於該UE策略資訊的。

【第18項】 一種用於由一安全錨功能單元（SEAF）進行無線通訊的方法，包括以下步驟：

藉由將網路策略資訊輸入一金鑰推導函數（KDF）來產生用於一網路節點的一金鑰，其中該金鑰可以用於在一使用者設備（UE）與該網路節點之間建立一安全連接；及

向該網路節點發送該金鑰。

【第19項】 根據請求項18之方法，亦包括以下步驟：在產生該金鑰之前參與同該UE的一認證程序或註冊程序中的至少一項，其中該參與包括：建立要在該UE與該SEAF之間共享的一錨金鑰。

【第20項】 根據請求項19之方法，其中該金鑰是進一步基於以下各項中的至少一項來產生的：該錨金鑰，或者該網路策略資訊有效的一時間量。

【第21項】 根據請求項20之方法，亦包括以下步驟：

向該網路節點發送以下各項中的至少一項：該網路策略資訊，或者該網路策略資訊有效的該時間量。

【第22項】 根據請求項18之方法，其中該網路策略資訊包括關於該網路節點是否在該網路中與該SEAF共置的一指示。

【第23項】 根據請求項18之方法，其中該網路策略資訊包括該網路節點的一安全級別。

【第24項】 根據請求項18之方法，其中該網路策略資訊包括關於該網路中的一通信期管理功能單元(SMF)是否要產生用於該UE與該網路之間的一通訊通信期的一通信期管理符記並且向該UE發送該通信期管理符記的一指示。

【第25項】 根據請求項18之方法，亦包括以下步驟：接收包括該UE的策略資訊的一訊息，其中該UE策

略資訊包括以下各項中的至少一項：UE能力資訊，或者UE安全資訊。

【第26項】 根據請求項25之方法，其中該金鑰是進一步基於該UE策略資訊來產生的。

【第27項】 根據請求項25之方法，其中該訊息包括一註冊訊息或者一附著請求訊息。

【第28項】 根據請求項25之方法，其中該網路策略資訊是基於該UE策略資訊來決定的。

【第29項】 根據請求項18之方法，其中該網路節點是該網路中的一存取和行動性管理功能單元（AMF）。

【第30項】 一種使用者設備（UE），包括：

一記憶體，用於儲存指令；及

一處理器，其中當該處理器執行該等指令時，該處理器經配置以進行以下操作：

接收用於與一網路建立一安全連接的一第一訊息，其中該第一訊息包括網路策略資訊；

藉由一金鑰推導函數（KDF）來產生一第一金鑰，其中該網路策略資訊是導入該KDF的一輸入；及

至少部分地基於該第一金鑰來驗證該網路策略資訊。

【第31項】 根據請求項30之UE，其中該處理器經配置以藉由以下操作來驗證該網路策略資訊：部分地基

於該第一金鑰來決定該第一訊息是否是有效的。

【第32項】 根據請求項31之UE，其中：

該第一訊息是利用從一第二金鑰推導出的一保護金鑰來進行完整性保護的；及

該處理器經配置以藉由以下操作來決定該第一訊息是否是有效的：基於該第一金鑰來執行對該第一訊息的完整性驗證。

【第33項】 根據請求項31之UE，其中該處理器經配置以進行以下操作：

若該決定是該第一訊息是有效的，則與該網路建立一安全連接。

【第34項】 根據請求項30之UE，其中該處理器經配置以進行以下操作：

進一步基於該UE與該網路中的一安全錨功能單元（SEAF）之間共享的一錨金鑰來產生該第一金鑰。

【第35項】 根據請求項34之UE，其中該處理器經配置以進行以下操作：

在接收該第一訊息之前執行與該SEAF的一認證程序或註冊程序中的至少一項，其中該錨金鑰是基於該認證程序或註冊程序中的至少一項來建立的。

【第36項】 根據請求項30之UE，其中該網路策略資訊包括一存取和行動性管理功能單元（AMF）的一安

全級別。

【第37項】 根據請求項30之UE，其中：

該第一訊息是從該網路中的一存取和行動性管理功能單元（AMF）接收的；及

其中該處理器經配置以藉由以下操作來建立該安全連接：向該AMF發送一第二訊息。

【第38項】 根據請求項37之UE，其中：

該第一訊息是一安全模式命令（SMC）訊息；及

該第二訊息是一SMC完成訊息。

【第39項】 一種安全錨功能單元（SEAF），包括：

一記憶體，用於儲存指令；及

一處理器，其中當該處理器執行該等指令時，該處理器經配置以進行以下操作：

藉由將網路策略資訊輸入一金鑰推導函數（KDF）來產生用於一網路節點的一金鑰，其中該金鑰可以用於在一使用者設備（UE）與該網路節點之間建立一安全連接；及

向該網路節點發送該金鑰。

【第40項】 根據請求項39之SEAF，其中該處理器經配置以進行以下操作：

在產生該金鑰之前參與同該UE的一認證程序或註冊程序中的至少一項，其中該參與包括：建立要在該

UE與該SEAF之間共享的一錨金鑰。

【第41項】 根據請求項40之SEAF，其中該處理器經配置以進行以下操作：

進一步基於該錨金鑰來產生該金鑰。

【第42項】 根據請求項39之SEAF，其中該處理器經配置以進行以下操作：

向該網路節點發送該網路策略資訊。

【第43項】 根據請求項39之SEAF，其中該網路策略資訊包括關於該網路節點是否在該網路中與該SEAF共置的一指示。

【第44項】 根據請求項39之SEAF，其中該網路策略資訊包括該網路節點的一安全級別。

【第45項】 根據請求項39之SEAF，其中該處理器經配置以進行以下操作：

接收包括該UE的策略資訊的一訊息，其中該UE策略資訊包括以下各項中的至少一項：UE能力資訊，或者UE安全資訊。

【第46項】 根據請求項45之SEAF，其中該訊息包括一註冊訊息或者一附著請求訊息。

【第47項】 根據請求項39之SEAF，其中該網路節點是一存取和行動性管理功能單元（AMF）。

【發明圖式】

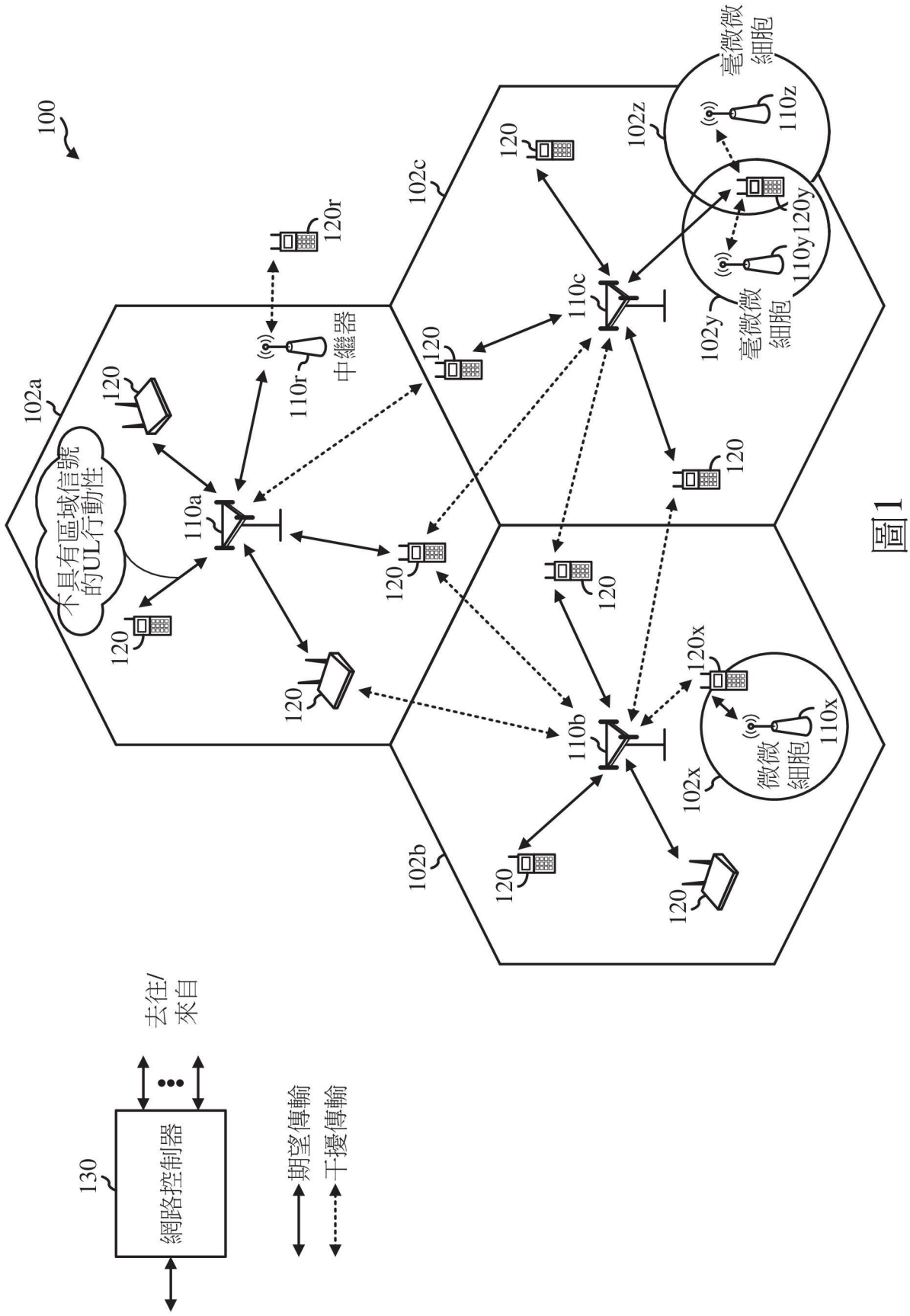
100
102a
102b
102c
102x
102y
102z
110a
110b
110c
110r
110x
110y
110z
120
120r
120x
120y
中繼器
不具有區域信號的UL行動性
毫微微細胞
微微細胞
130
網路控制器
去往/來自
期望傳輸
干擾傳輸

圖1

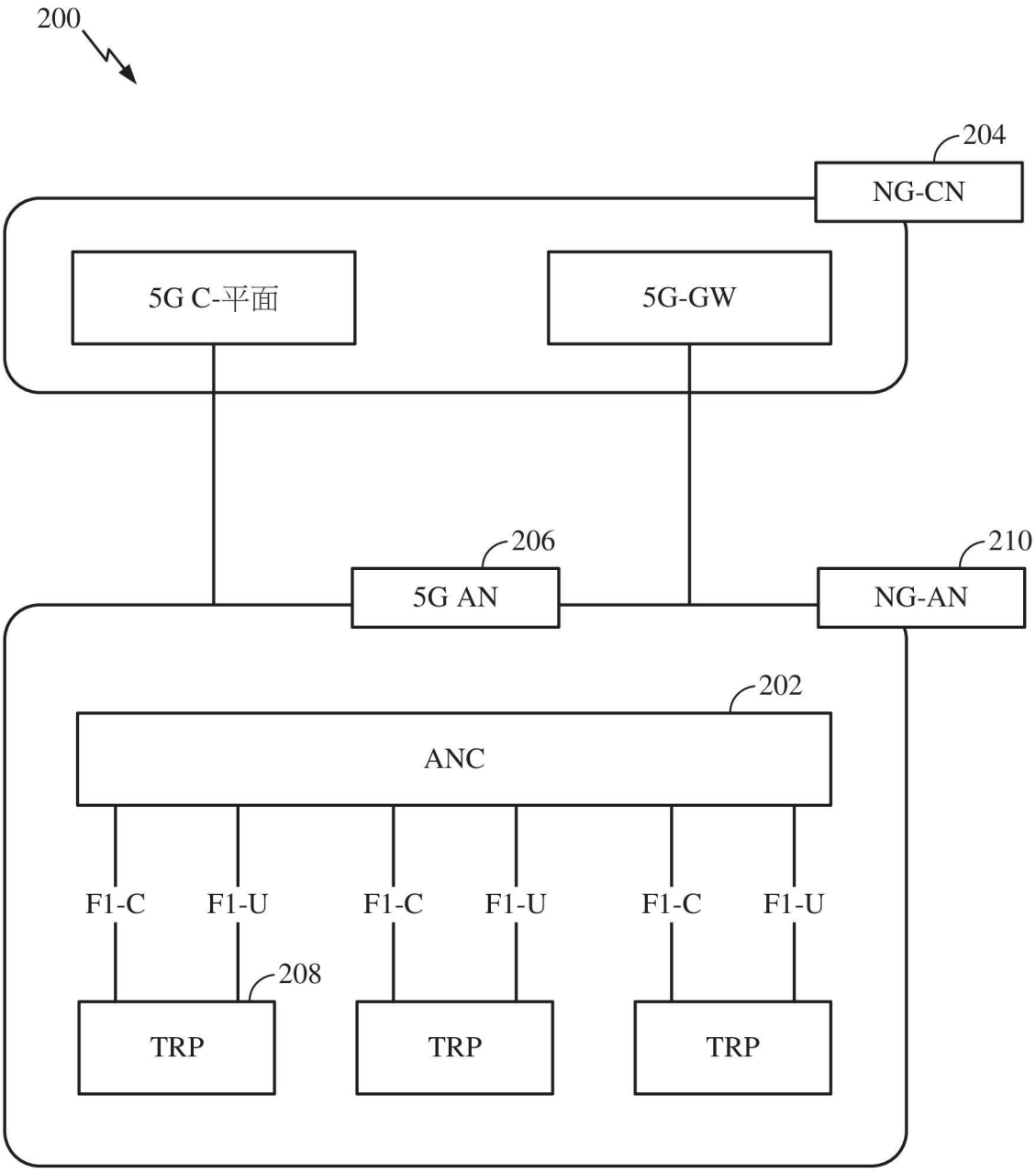
200
204
NG-CN
5G C-平面
5G-GW
206
5G AN
210
NG-AN
202
ANC
F1-C
F1-U
F1-C
F1-U
F1-C
F1-U
208
TRP
TRP
TRP

圖2

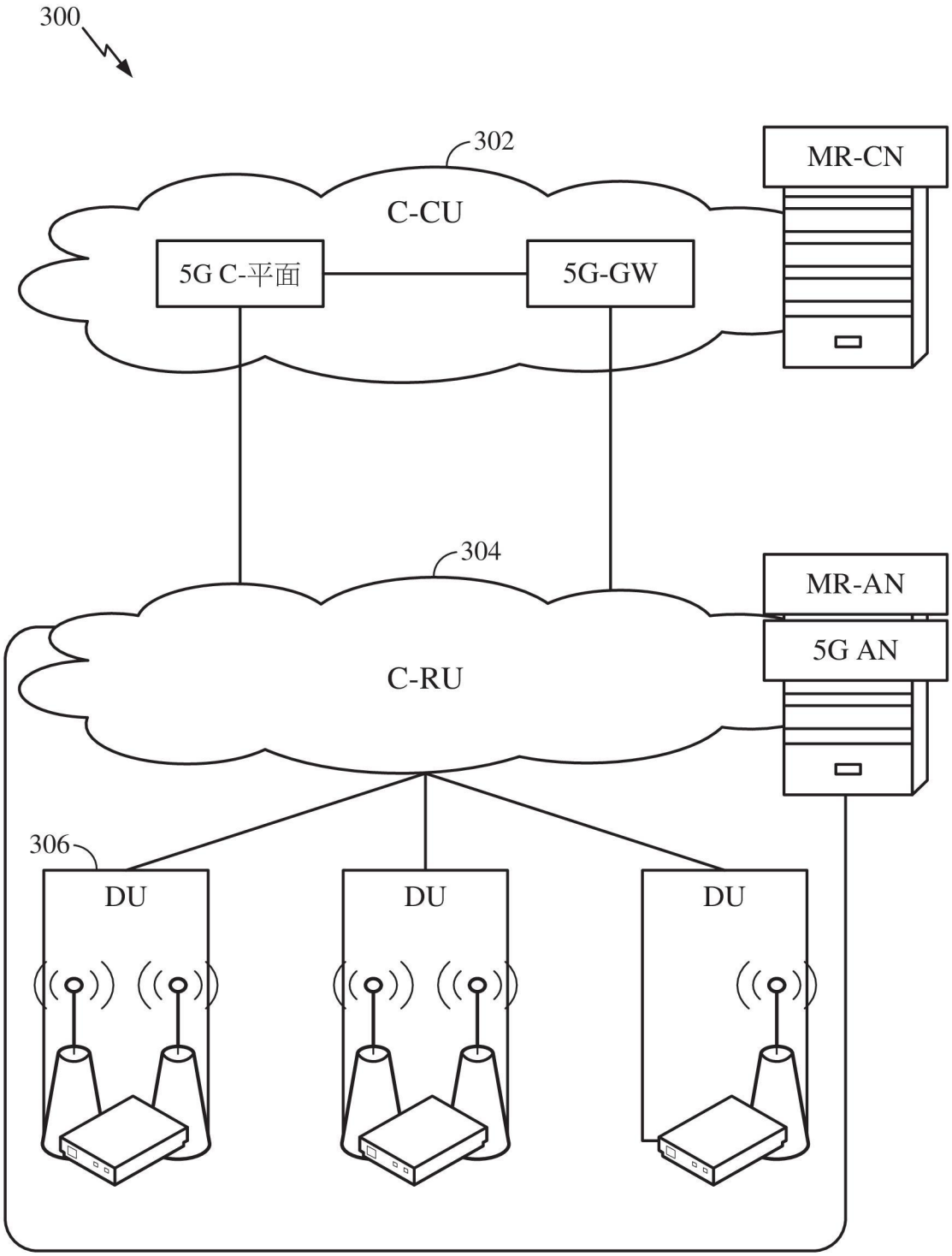

圖3

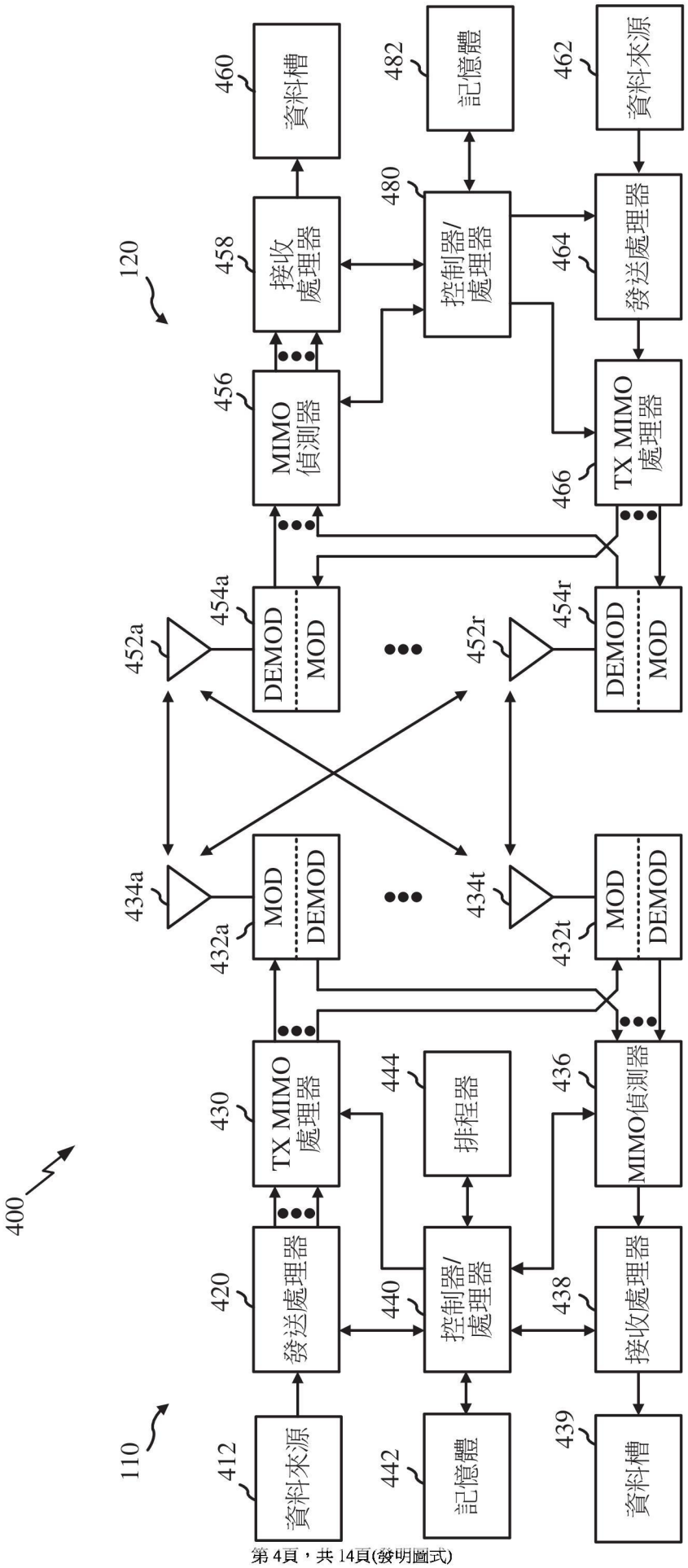
400
110
120
412
資料來源
420
發送處理器
430
TX MIMO 處理器
434a
434t
432a
MOD
DEMOD
432t
452a
452r
454a
454r
DEMOD
MOD
456
MIMO 偵測器
458
接收 處理器
460
資料槽
440
控制器/ 處理器
442
記憶體
444
排程器
480
控制器/ 處理器
482
記憶體
436
MIMO偵測器
438
接收處理器
439
資料槽
462
資料來源
464
發送處理器
466
TX MIMO 處理器

圖4

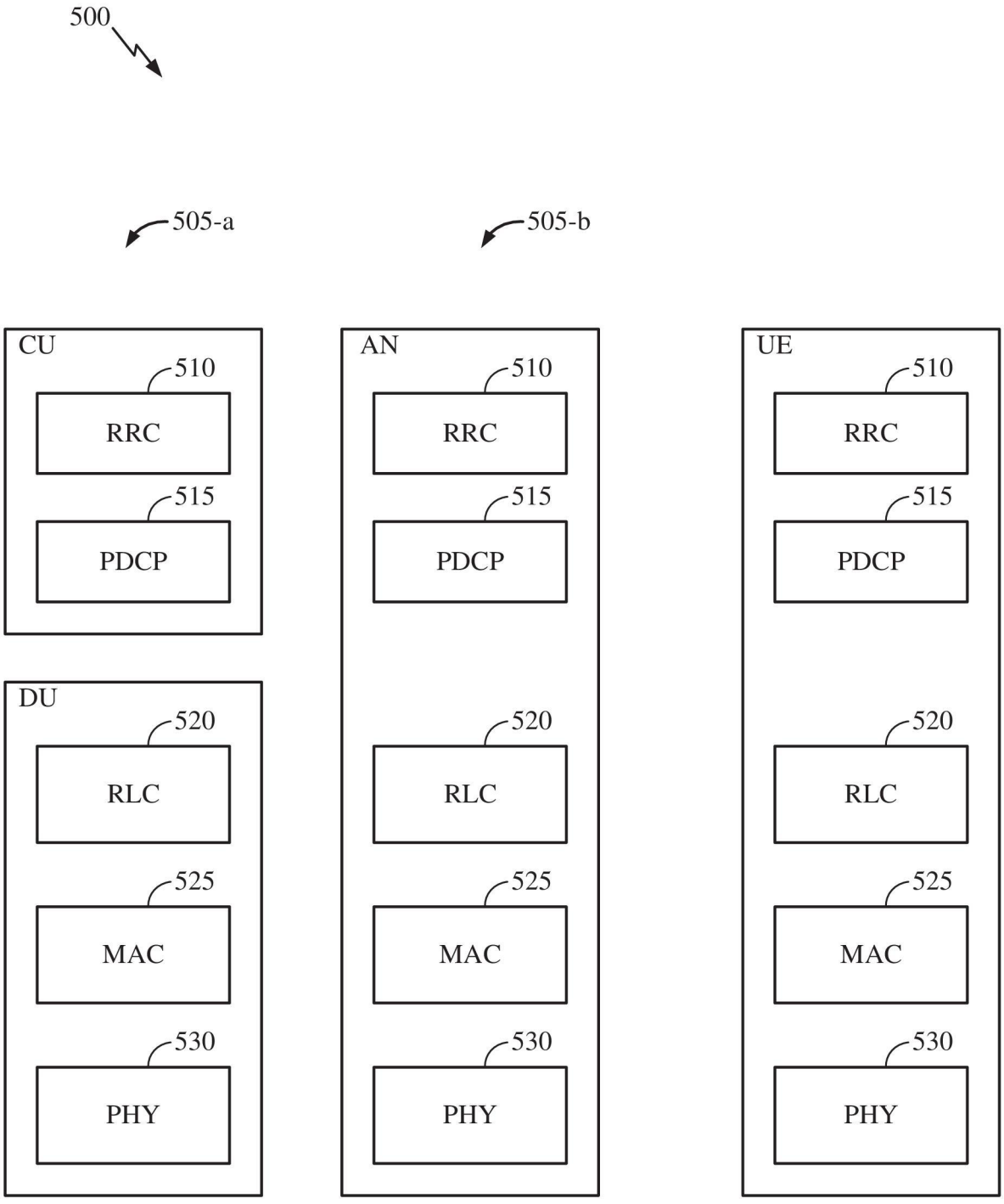
500
505-a
505-b
CU
510
RRC
515
PDCP
DU
520
RLC
525
MAC
530
PHY
AN
510
RRC
515
PDCP
520
RLC
525
MAC
530
PHY
UE
510
RRC
515
PDCP
520
RLC
525
MAC
530
PHY

圖5

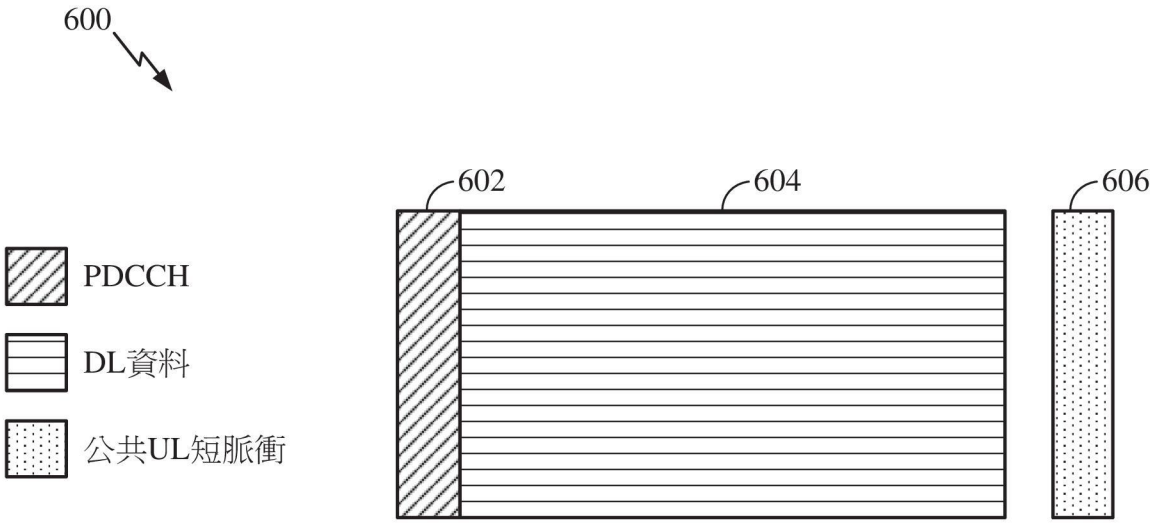
600
602
604
606
PDCCH
DL資料
公共UL短脈衝

圖6

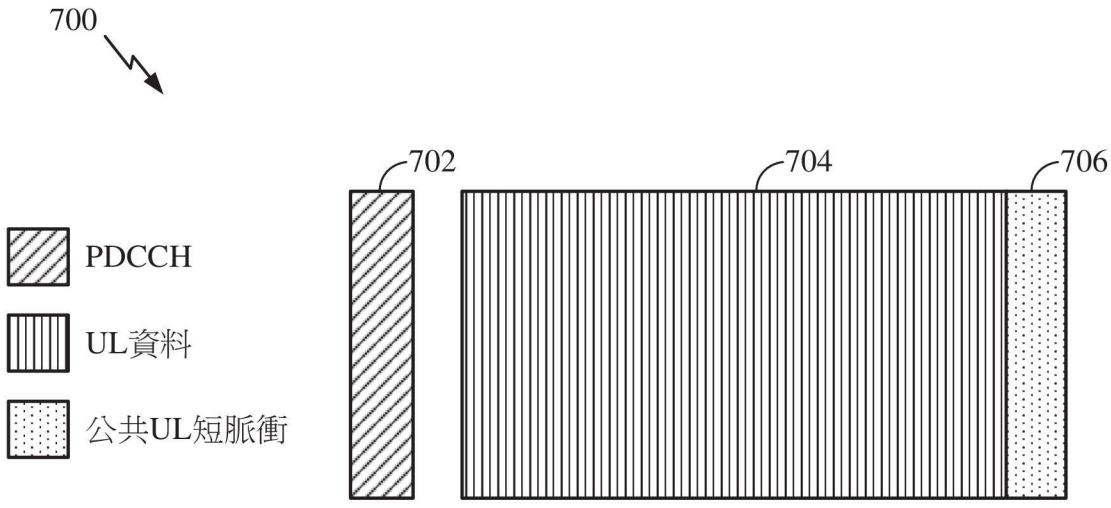
700
702
704
706
PDCCH
UL資料
公共UL短脈衝

圖7

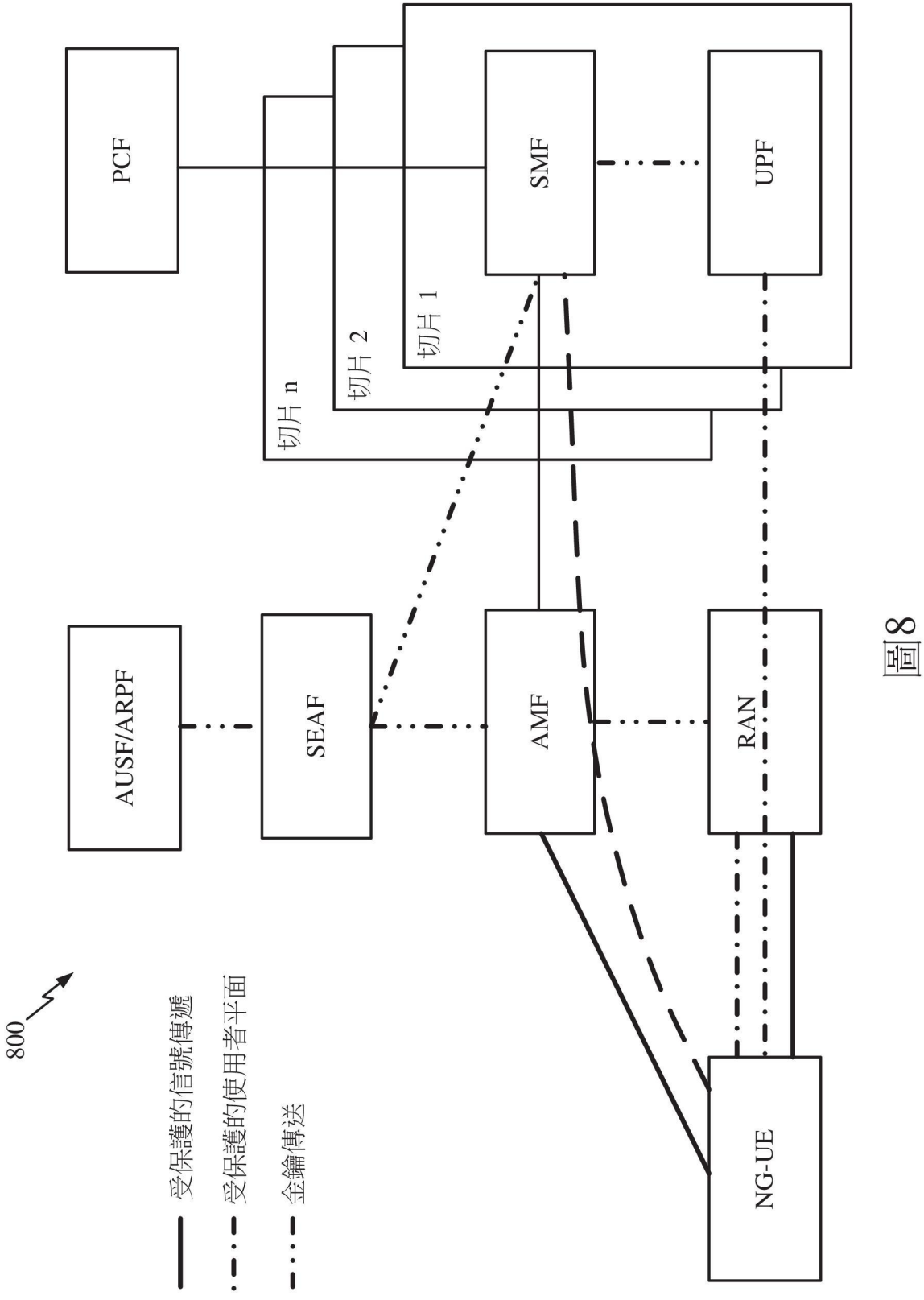
PCF
SMF
UPF
切片 1
切片 2
切片 n
AUSF/ARPF
SEAF
AMF
RAN
NG-UE
800
受保護的信號傳遞
受保護的使用者平面
金鑰傳送

圖8

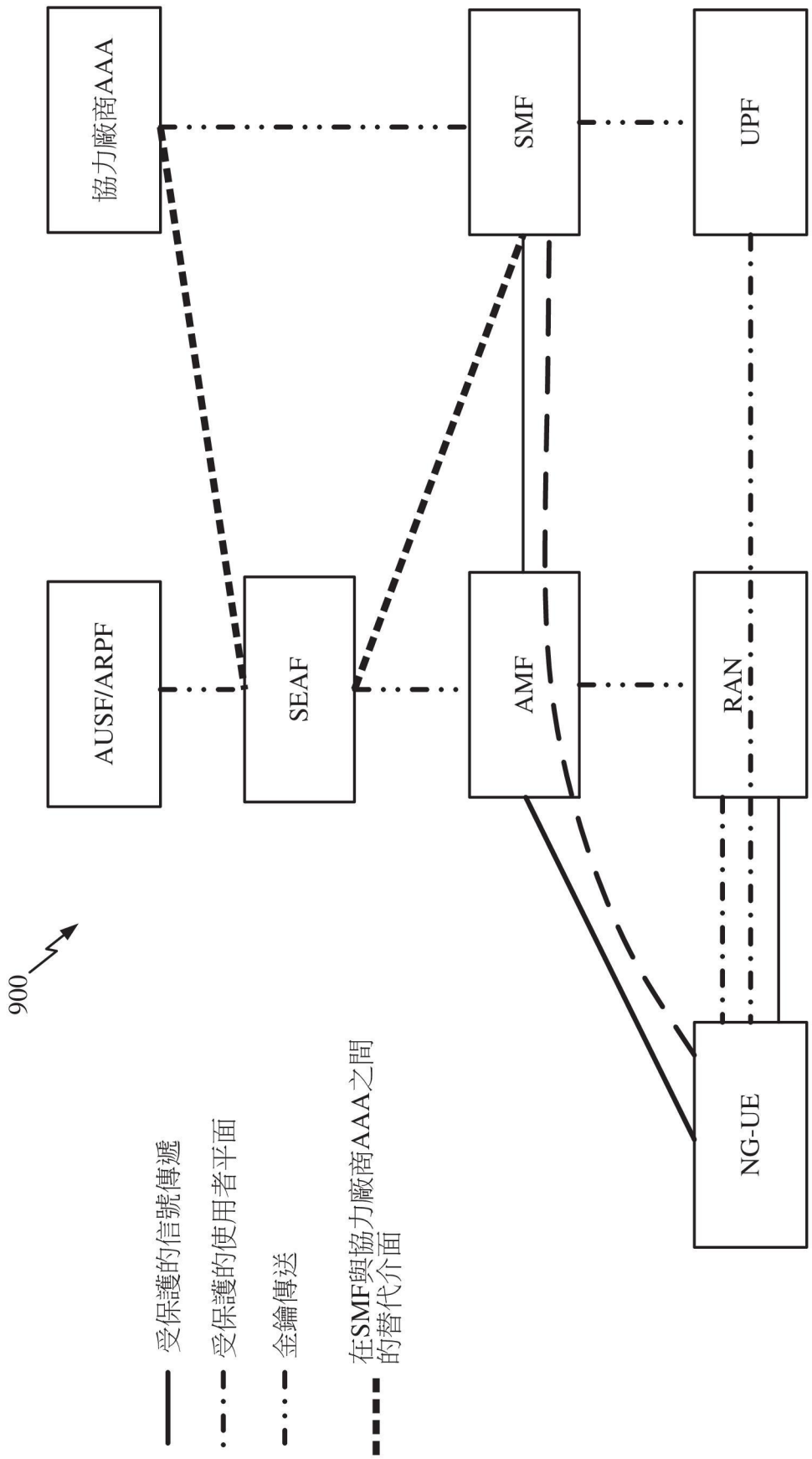
協力廠商AAA
SMF
UPF
AUSF/ARPF
SEAF
AMF
RAN
NG-UE
900
受保護的信號傳遞
受保護的使用者平面
金鑰傳送
在SMF與協力廠商AAA之間的替代介面

圖9

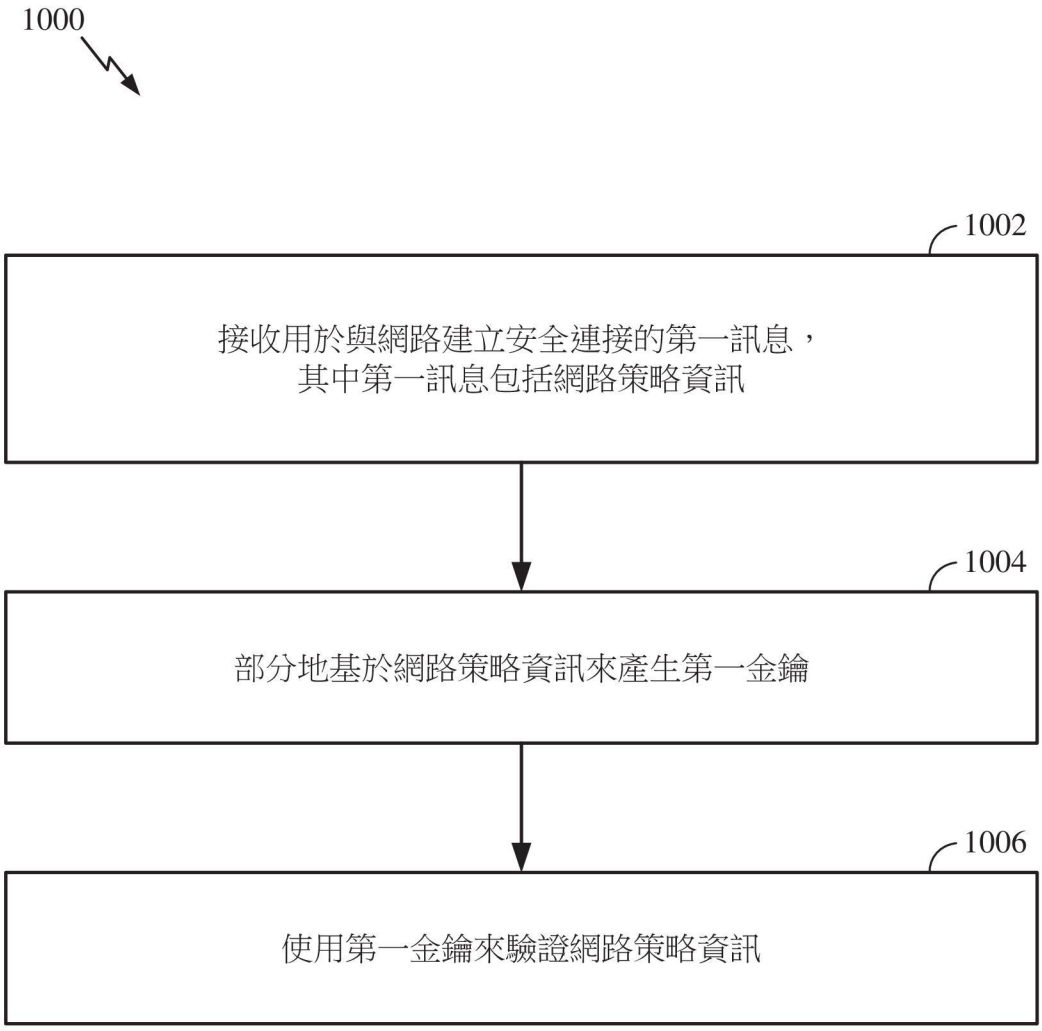
1000
1002
接收用於與網路建立安全連接的第一訊息，
其中第一訊息包括網路策略資訊
1004
部分地基於網路策略資訊來產生第一金鑰
1006
使用第一金鑰來驗證網路策略資訊

圖10

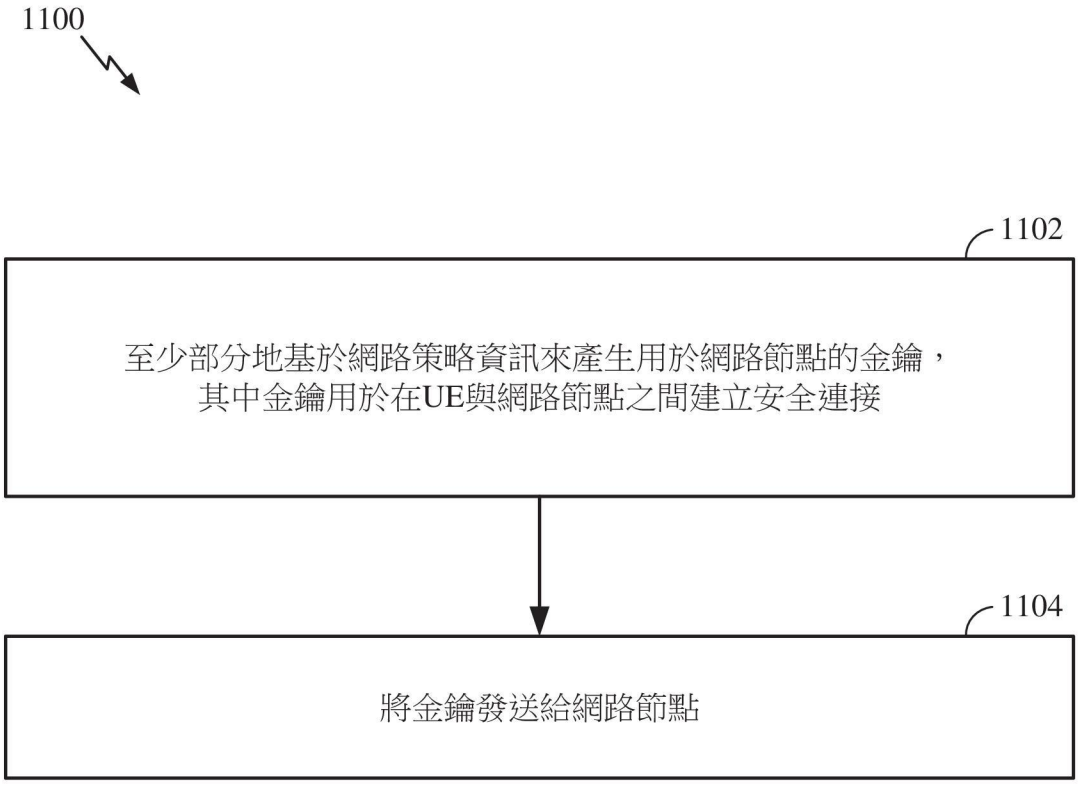
1100
1102
至少部分地基於網路策略資訊來產生用於網路節點的金鑰，
其中金鑰用於在UE與網路節點之間建立安全連接
1104
將金鑰發送給網路節點

圖11

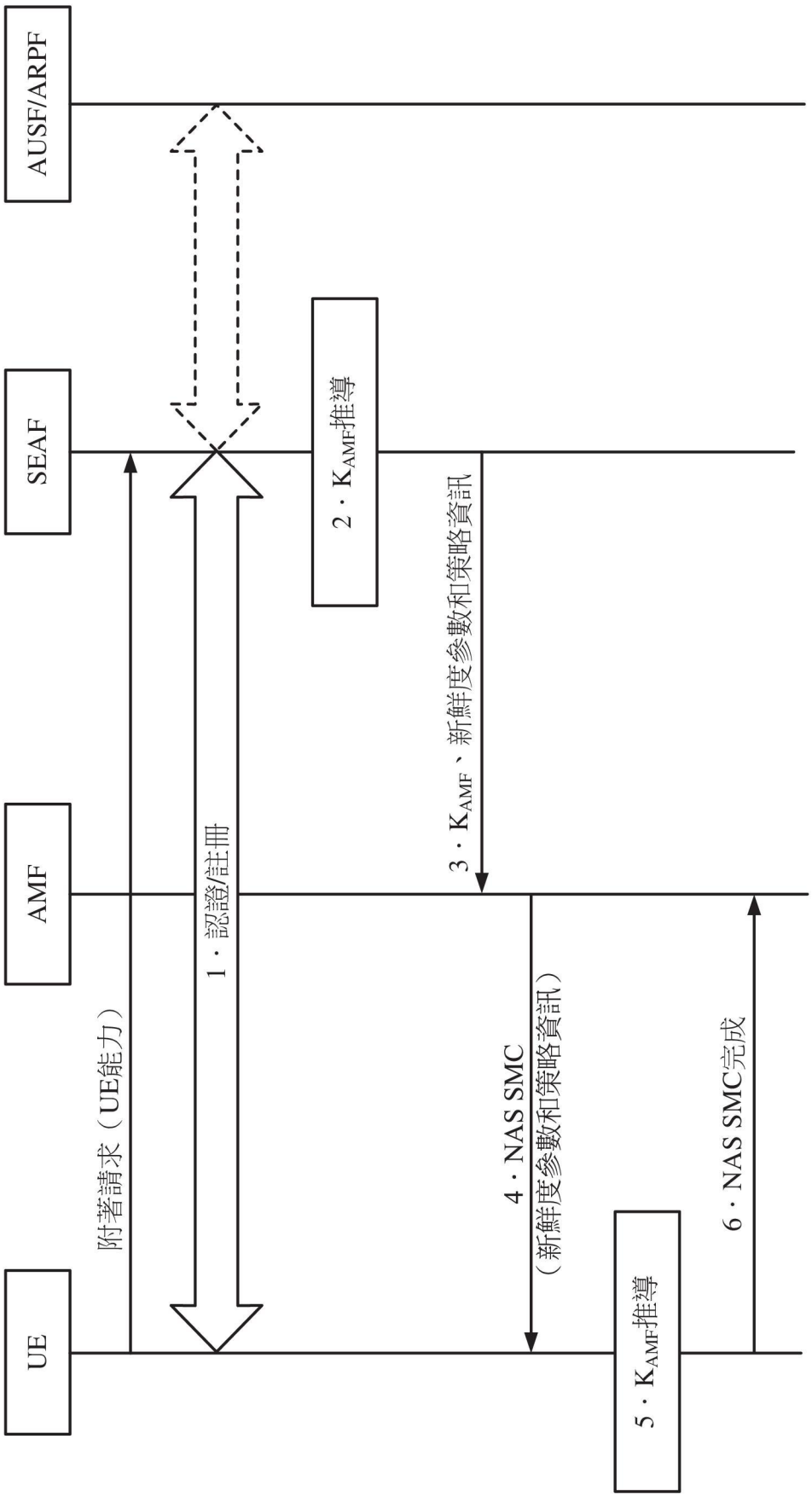
AUSF/ARPF
SEAF
AMF
UE
2．K_{AMF}推導
1．認證/註冊
3．K_{AMF}、新鮮度參數和策略資訊
附著請求（UE能力）
4．NAS SMC
（新鮮度參數和策略資訊）
5．K_{AMF}推導
6．NAS SMC完成

圖12

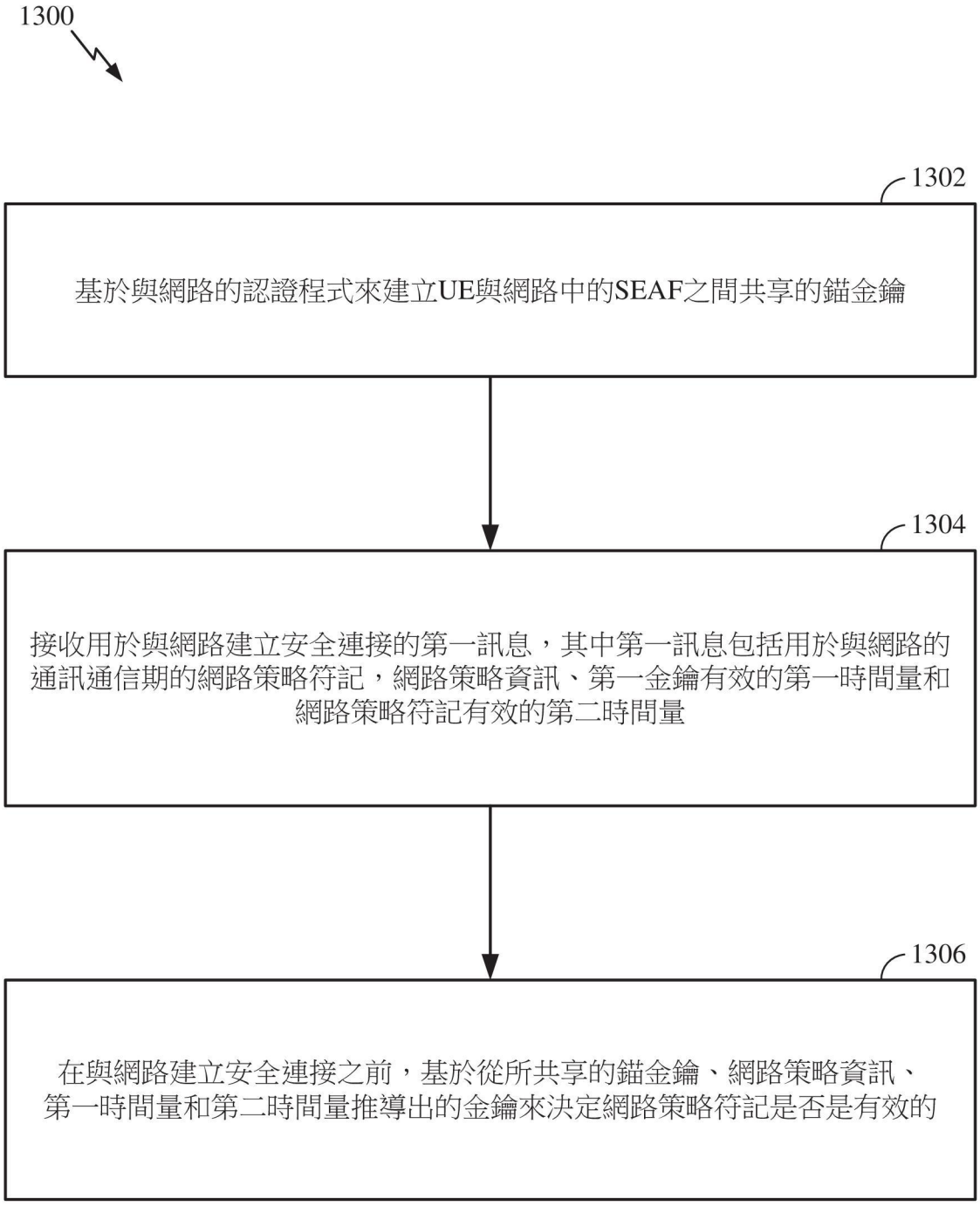
1300
1302
基於與網路的認證程式來建立UE與網路中的SEAF之間共享的錨金鑰
1304
接收用於與網路建立安全連接的第一訊息，其中第一訊息包括用於與網路的通訊通信期的網路策略符記，網路策略資訊、第一金鑰有效的第一時間量和網路策略符記有效的第二時間量
1306
在與網路建立安全連接之前，基於從所共享的錨金鑰、網路策略資訊、第一時間量和第二時間量推導出的金鑰來決定網路策略符記是否是有效的

圖13

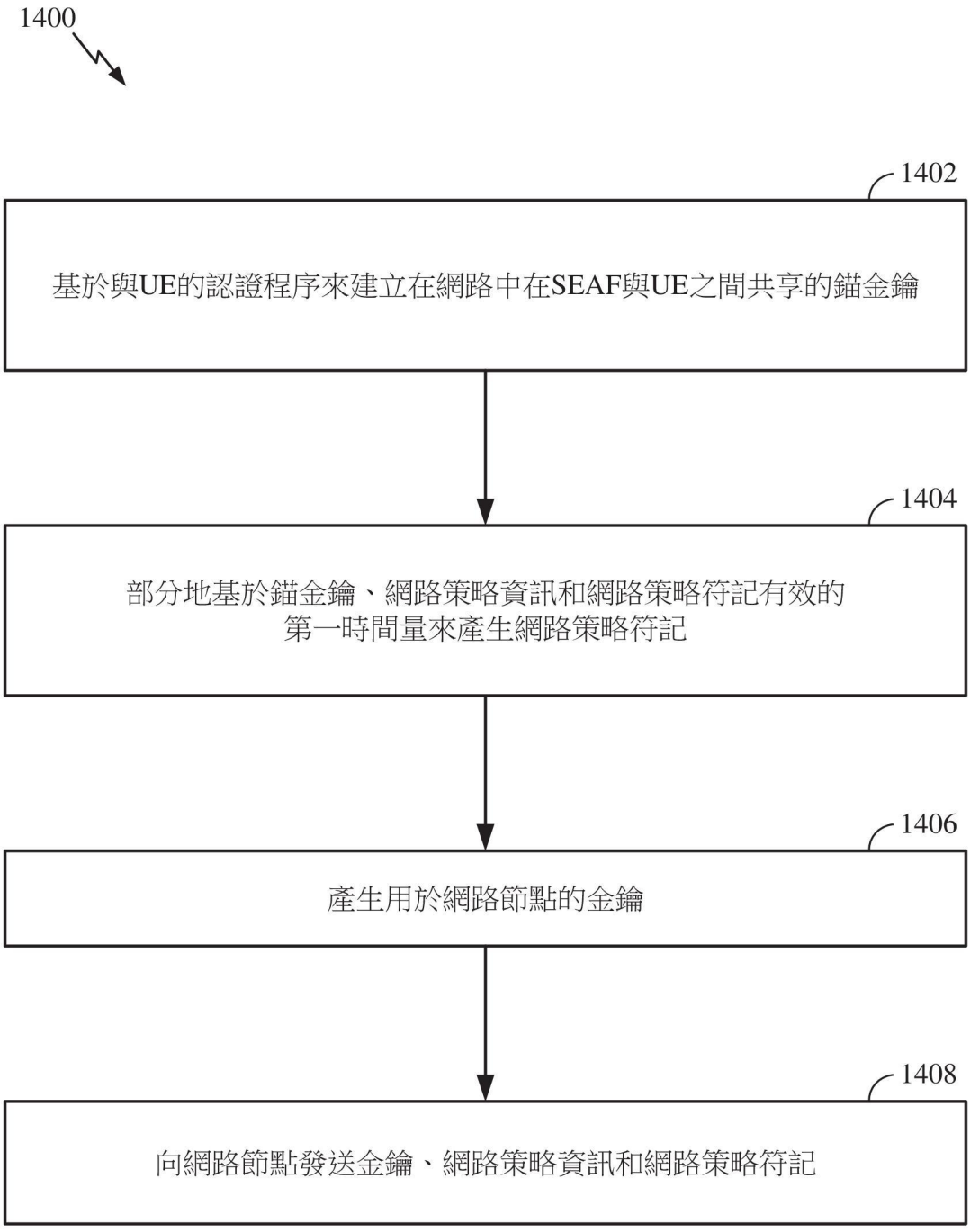
1400
1402
基於與UE的認證程序來建立在網路中在SEAF與UE之間共享的錨金鑰
1404
部分地基於錨金鑰、網路策略資訊和網路策略符記有效的
第一時間量來產生網路策略符記
1406
產生用於網路節點的金鑰
1408
向網路節點發送金鑰、網路策略資訊和網路策略符記

圖14

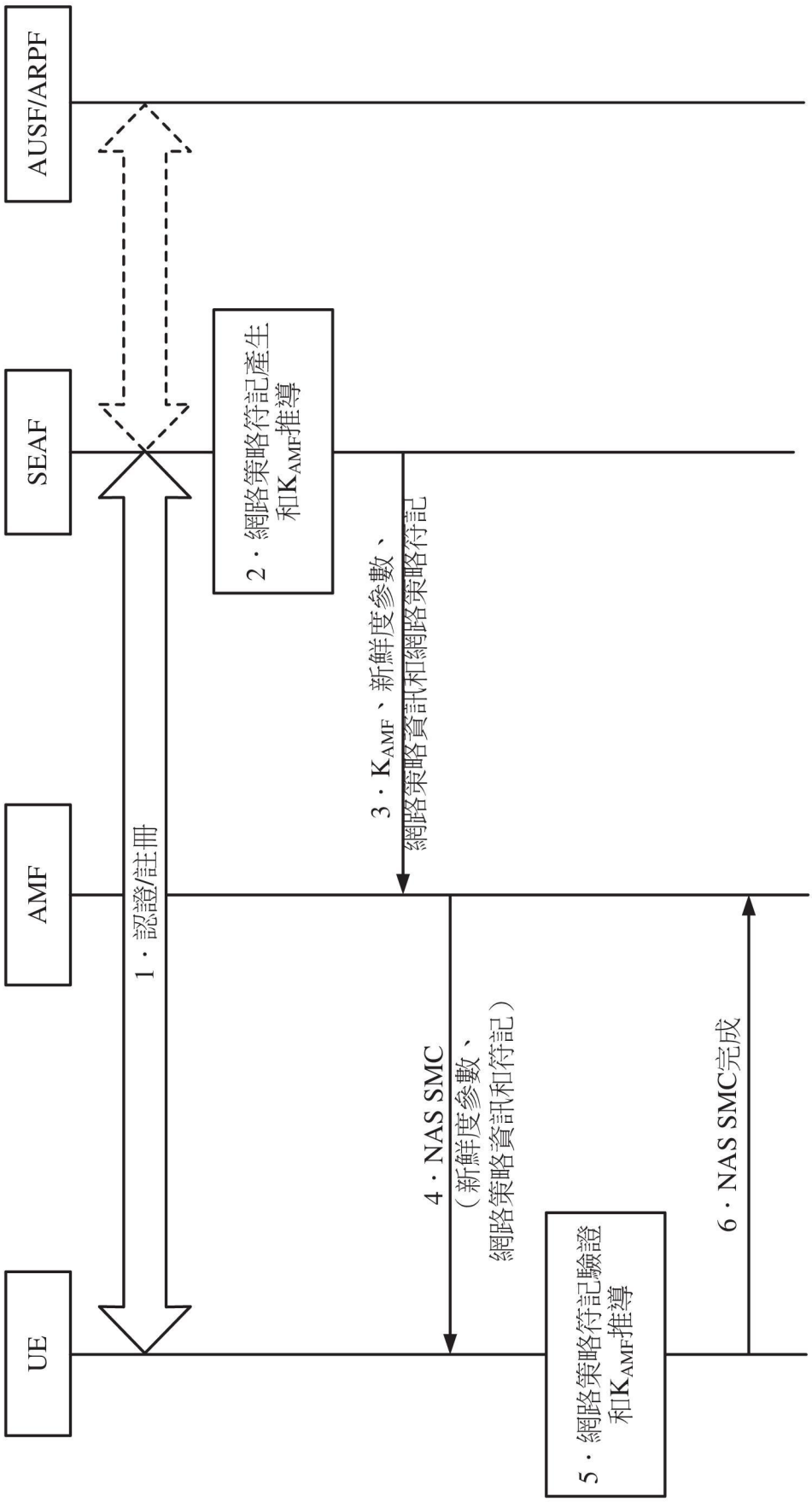
AUSF/ARPF
SEAF
AMF
UE
1．認證/註冊
2．網路策略符記產生
和K_{AMF}推導
3．K_{AMF}、新鮮度參數、
網路策略資訊和網路策略符記
4．NAS SMC
（新鮮度參數、
網路策略資訊和符記）
5．網路策略符記驗證
和K_{AMF}推導
6．NAS SMC完成

圖15