I493952

103 年 4 月 30 日修正替換頁

發明專利說明書

公告本

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：096149792

※ 申請日期： 96 年 12 月 24 日

※IPC 分類：

H04L 9/14 (2006.01)

H04W 92/00 (2009.01)

一、發明名稱：（中文/英文）

基地台自行配置方法及裝置/Method and Apparatus for Base Station Self-Configuration

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

無線創新信號信託公司/ Signal Trust for Wireless Innovation

代表人：（中文/英文）布魯斯・伯恩斯坦/Bruce G. BERNSTEIN

住居所或營業所地址：（中文/英文）

美國德拉瓦州 19805 威明頓中央路 1011 號 327 室/1011 Centre Road, Suite 327, Wilmington, DE 19805, U.S.A.

國　籍：（中文/英文） 美國/ US

三、發明人：（共 4 人）

1. **姓　名：**彼得・王/Peter S. WANG
   國　籍：美國/US
2. **姓　名：**路易斯・顧吉恩/Louis J. GUCCIONE
   國　籍：美國/US
3. **姓　名：**詹姆斯・米勒/James M. MILLER
   國　籍：美國/US
4. **姓　名：**烏利斯・奧維拉-赫恩安德茨/Ulises OLVERA-HERNANDEZ
   國　籍：墨西哥/MX

送件申請修正之日期：103 年 10 月 1 日

103年10月01日修正替換頁

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國 US；2006/12/27；60/882,079

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

送件申請修正之日期：103 年 10 月 1 日

五、中文發明摘要：

公開了一種用於無線通信中基地台的操作的方法和設備，包括配置用於與其他基地台進行安全和已驗證的通信的基地台。

六、英文發明摘要：

Disclosed is method and apparatus for operation of a base station in wireless communications, including configuration of the base station for secure and authenticated communications with other base stations.

送件申請修正之日期：103 年 10 月 1 日

103年10月01日修正替換頁

七、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:

無

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

送件申請修正之日期：103 年 10 月 1 日

九、發明說明：

【技術領域】

本發明涉及無線通信。更特別地，本發明涉及無線通信中的基地台的自配置和安全特性。

【先前技術】

為了提供改善的頻譜效率和更快的使用者體驗，第三代合作夥伴計畫（3GPP）已經啟動了長期演進（LTE）項目以將新的技術、新的網路架構、新的配置、新的應用和新的服務引入到無線行動網路中。

雖然對更強功能性的需求在繼續，但也同時需要低維護 LTE 系統，特別是在網路部署和操作時間優化方面。

在 LTE、3GPP 通用移動電信系統（UMTS）系統前使用的通用移動電信系統地面無線接取網路（UTRAN）架構如第 1 圖所示。核心網 100 與包括多個無線電網路系統（RNS）120 的 UTRAN 110 進行通信。每一個 RNS 包括無線電網路控制器（RNC）130 和一個或多個 Node-B 135。所部署的 Node-B 135 的配置和操作完全由 RNC 130 通過 Iub 鏈路 140 並用顯式命令來控制。Iub 140 是先前已經定義的 RNC 到 Node-B 介面。Node-B 的配置和服務升級取決於 RNC 和其他胞元工程和計畫上的努力。在 LTE 之前，在 UTRAN Node-B 135 之間不存在連接，並且不存在自配置和優化的需要。不存在 Node-B 之間操作的自配置的裝置和被定義的過程。

在新的 LTE 網路系統中，如第 2 圖所示，E-UTRAN

架構已經被改變。以前的 RNC 節點不再存在。演進型 Node-B（eNB）200、205 執行用於 E-UTRAN 210 的無線電存取網路功能，直接與核心網（EPC）220 鏈結，並且在其自身之間被鏈結。在 E-UTRAN 中，新的 eNB 200、205 承擔 RAN 配置、操作和管理控制功能以及無線電介面配置和操作。更進一步地，每一個新的 eNB，如 200，現在通過 S1 介面直接與 LTE 核心網 220 交互作用，同時也通過 X2 介面 240 和 X2 連接控制（X2C）介面（未示出）與相鄰 eNB 205 交互作用，用以代表新的 E-UTRAN 來處理無線傳輸/接收單元（WTRU）移動性管理任務。

當新被部署的 eNB 200、205 加電時，其執行自配置任務，包括通過 X2C 介面操作以與相鄰操作的 eNB 交互作用。這一初始交互作用被用於採集資訊來認證 eNB 並當 eNB 自身準備好進入 E-UTRAN 操作模式以服務在其覆蓋區域中的 WTRU 時，啟動配置和協作。

【發明內容】

本發明涉及在自配置階段通過基地台之間的連接的操作過程。

公開了用於自配置基地台以及與相連的相鄰基地台之間通信的操作。新近被部署的基地台執行自配置以將其自身與其相鄰操作的基地台或胞元相關聯。安全過程被執行以保護網路免受特定的攻擊。

【實施方式】

下文引用的術語“無線傳輸/接收單元（WTRU）”包

括但不局限於使用者設備（UE）、移動站、固定或移動使用者單元、傳呼機、行動電話、個人數位助理（PDA）、電腦或能在無線環境中工作的其他任何類型的使用者設備。下文引用的術語“基地台”包括但不局限於 Node-B、站點控制器、存取點（AP）或是能在無線環境中工作的其他任何類型的周邊設備。

儘管這裏描述的實施方式是以 LTE 為實施環境的，但這些實施方式應該被作為示例，並且不限於這一特定的無線技術。

第 3-6 圖描述了發生在自配置 eNB、連接到該自配置 eNB 的（也就是“相鄰的”）eNB 及存取閘道中的事件的時間序列。序列按時間進度從最上面向下開始。在相同水準級別的事件是同時發生的。

參考第 3 圖，當自配置 eNB 加電時，其 S1 介面較佳地被首先加電 305。通用網際協議（IP）功能或 eNB 特定 IP 地址解析功能通過 S1 介面獲得用於自配置 eNB 的唯一的 IP 地址 300。然後，自配置 eNB 將以其主要運營商的服務存取閘道（aGW）310 來執行 eNB 網路驗證。

當自配置 eNB 已經成功通過網路驗證時，隨後該 eNB 加電並用其 IP 位址初始化 320，該 IP 位址通過 S1 介面或 X2 介面配置或者獲得，其中 S1 介面或 X2 介面將自配置 eNB 與其他相鄰 LTE eNB 相連接。

如可選的早期動作，eNB 隨後獲取其連接 X2 的相鄰 eNB 的標識，例如，其 eNB-Id 和/或胞元-Id、公共陸地移

動網路（PLMN）-Id330 和諸如當前操作狀態 330 的其他的非機密資訊。然後 eNB 可以通知服務 aGW 以便 eNB 獲得與連接 X2 的相鄰 eNB 相關的必要的網路指示和/或驗證，以用於驗證和許可操作，如 WTRU 切換或 eNB 測量和報告重獲。儘管這一可選的早期動作 330 在第 3 圖中以“同步交換（handshake）”顯示，其也可以是如第 7 圖中顯示的一對請求和回應消息或任何其他合適的過程。將為這樣的資訊聯繫的相鄰 eNB 是那些被配置在默認相鄰 eNB 列表中的 eNB，例如那些保存在 UMTS 積體電路卡（UICC）設備中的 eNB。

這一用於早期動作的方法使得網路在多賣方/多運營商環境中通過 E-UTRAN 間的操作來維持特定的輸入或控制。首先，這種處理允許 eNB 從那些在與預先配置的相鄰 eNB 列表比較而作出回應的 eNB 處收集精確的相鄰 eNB 資訊，以便 eNB 可以通知網路/EPC 關於新的 eNB 和其連接的鄰居以及它們實際的操作狀態。第二，eNB 可以從網路獲取關於相鄰 LTE eNB 的 X2C 介面的策略的操作指南，這是因為相鄰 eNB 可能或不可能屬於相同的網路提供商/運營商。eNB 也可以獲取其他重要的操作資訊。

通過其相鄰非機密資訊的自配置 eNB 的單向可選收集不包括敏感資訊重獲。當 eNB 間的驗證和安全鑰匙關聯已經發生時，由 eNB 從其鄰居進行的敏感資訊的收集發生在一個較晚階段。

在初始資料收集後，eNB 將隨後通過 S1 發送

E-UTRAN 參數請求 340 和其在上面早期 X2C 步驟公開的資訊。可替換地，如果不採取早期的 X2C 動作，eNB 將通過 S1 發送請求（Request）。在 E-UTRAN 參數請求被傳輸到服務 aGW 後，自配置 eNB 獲取 350 需要的操作參數以用於 E-UTRAN，包括通過 X2C 的用於 eNB 間驗證和安全鑰匙協議過程，例如通用 eNB 證書、通用 eNB 共用密鑰、將使用的 eNB 間安全演算法以及通用 eNB 安全鑰匙集。

在 X2C 上對驗證、完整性和機密性保護的需要已經在先前被存檔。輕權重的驗證，這裏定義為 eNB 間驗證，並且完整性和/或加密鑰匙協議，在這裏被定義為安全鑰匙關聯過程，這些在下面被描述以用於在任何一對 eNB 之間的 LTE eNB 間驗證和安全鑰匙關聯，包括在自配置 eNB 和其已部署的可操作的相鄰 eNB 之間。

注意到在 eNB 自配置中的 eNB 間驗證過程需要確定在節點級別處 eNB 對的可靠性。下面執行的沒有節點級別控制的驗證和節點級別參數的參與將不能保證相同級別的 eNB 可靠性。

公開了兩種實施方式，一種利用有改進的基本的網際協議安全（IPsec），及一種用於在“手動”模式下與基本的 IPsec 在 eNB 級別上直接進行交互作用作用。

第一種實施方式利用用於 LTE 的基本的網際協議安全 eNB-eNB 通信，並且在標準 TCP/IP 協定組周圍被構造。對現有的網際協議安全和其潛在的弱勢的理解對於這

一實施方式的新穎性評價有幫助，並且因此這裏隨後進行了描述。

在 TCP/IP 協定中，IP 標頭資訊的域保護在阻止導致位址欺騙和經常引發會話劫持的典型攻擊方面是十分重要的。這樣，網路層驗證和機密性利用一組網際網路工程任務組（IETF）標準化的過程被應用，該過程被稱為網際協議安全（IPSec）。驗證，在上下文中意味著資料完整性和源位址保護，當沒有機密性（加密）來說時，驗證對於 IPSec 來說是強制的。

IPSec 的三個基本組成為驗證保護、機密保護和安全關聯。驗證和機密保護機制經由在 IP 封包中的附加欄位被實施。在 IPSec 中是強制的用於驗證的欄位為驗證標頭（AH）。該欄位被放置在緊接著 IP 標頭。這一欄位包括說明將使用的加密演算法、用於重新阻止的序列號和提到的作為完整性校驗值（ICV）的完整性散列的各種子欄位。

跟著驗證欄位的機密性欄位是可選的並且被稱為封裝安全有效載荷（ESP）。它包括與 AH 相似的子欄位：唯一加密演算法的說明，如 DES、AES、3DES 或 BLOWFISH，序列號子欄位，被加密的有效載荷資料，以及包括用以完整性保護被加密的資料的散列的子欄位。用於 ESP 使用的散列保護了僅被加密資料的完整性，而 AH 散列保護整個 IP 封包，如為 IPSec 所指示的，該 IP 封包總是包括 AH 欄位並有時包括 ESP 欄位。

與僅驗證相反，為確定是否驗證和機密性被使用，安

全關聯（SA）在 IPSec 中被設置。SA 包括三部分：安全演算法其他參數的說明、IP 目的地位址和用於 AH 或 ESP 的識別符。SA 通過網際鑰匙交換（IKE）協議被實施，如下所述。

在任何驗證/完整性和機密性可以在 IPSec 中被使用之前，密碼鑰匙、演算法和參數必須被協商。IKE 協定包括需要的協商的許多協定，並且 IKE 協定在多種情形中被使用。IKE 協定簡化的觀點被描述並且與以下的本發明所公開的相關。

在發起方和回應方之間的初始交換建立了初始的安全關聯。這些交換包括兩組請求/回應對或總共的四個消息。

第一對建立了密碼演算法的使用並且執行 Diffie-Hellman 交換以得出種子，從該種子中完整性和機密性鑰匙被推導出來。第二對使用從第一交換中生成的鑰匙來驗證第一組消息，交換標識並認證，並且提供用於接下來的子 SA 的建立。

協議的發起方（I）發送以下的有效載荷：

1. I → R: HDR_I, SA_I, g_I^x, N_I

回應方（R）用以下來回應：

2. R → I: HDR_R, SA_R, g_R^y, N_R

這是初始安全關聯中的第一對消息。HDR 包括標頭資訊，該標頭資訊主要維持在兩個實體之間的通信的狀態。SAI 和 SAR 是安全演算法和參數協商機制，其中發起方提出

一組選擇，從該組選擇中由回應方來選擇。為了處理 Diffie-Hellman 協議，值 和 被交換以產生共用的秘密值 ，該值作為種子來使用先前協商的演算法生成完整性和機密性鑰匙。品質 g 是迴圈組（階次 p-1）的生成元，其中 p 是非常大的起始號碼。值 p 和 g 是公知的，並且所有的計算以模 p 執行。最後，現時 NR 和 NI 被交換以阻止重複。

第二對消息是

3. I → R: HDR_I, SK{ID_I, $Cert_I$, AUTH, $SA2_I$, ..., 其他欄位以創造子 SA}

4. R → I: HDR_R, SK{ID_R, $Cert_R$, Sig_R, AUTH, $SA2_R$, ..., 其他欄位以創建子 SA}

消息 3 和 4 是從在 IETF 協議中規定的稍微簡化而來。該第二對使用從第一消息對得出的安全鑰匙資訊，如上面所陳述的。SK 指定在括弧（brace）內所顯示的變元上的安全鑰匙操作。兩個安全鑰匙，SK_a（驗證，這裏意味著完整）和 SK_e（加密）從 g^{xy}（來自 Diffie-Hellman）中被生成。它們分別被用於保護交換的完整和機密。發起方和回應方標識（ID_I 和 ID_R）和它們的相應標識秘密通過每一實體證明給其他；AUTH 包括用於每一方向的完整校驗值。認證（$Cert_I$ 和 $Cert_R$）提供與 SK_a 和 SK_e 分離的鑰匙資訊，以雙向檢驗 AUTH。

只要沒有消息 1 和 2 的偷聽發生，在發起方和回應方之間建立的 SA 對於將要發生的後來的子交換是安全的。

然而，這一初始消息對可能易受一種公知的“中間人攻擊（man-in-the-middle attack）”的侵襲，該攻擊者可以強迫每一有效實體使用它可以採用的鑰匙種子。這裏描述發起方和回應方之間的攻擊包括整個通信過程，其中攻擊器能夠假冒為每一個。

一種典型的在I和R之間的初始IKE交換的中間人攻擊如第6圖所示。在步驟1到4，A從I接收g_I^x和從R接收g_R^y；另外A發送g_R^m（其Diffie-Hellman值）到I和R，其中兩者都假設另外的一個而不是真正的創始方 A 是那值的創始方。已知每一方的資訊，則很容易顯示A分別與有效的交流者I和R共用Diffie-Hellman種子g^{mx}和g^{my}。當I使用g^{mx}並且相似地有R使用g^{my}時，A現在計算相同的加密（SK_e）和驗證/完整（SK_a）鑰匙。

在步驟5到8的SK功能不保護發送消息的完整或機密，假定A已經通過擾亂鑰匙的使用欺騙了通信，並且成功假冒了I和R。任何預先共用的密鑰資訊的缺席阻止在I和R之間的前兩個交換的保護。用於阻止這種類型的攻擊的方法和設備的實施方式在下面被描述。

第一種實施方式如第7圖所示，特徵600。在節點級別eNB_1和eNB_2（如自配置eNB和相鄰eNB，如上面所描述的和在第7圖種顯示的），eNB共用網路分佈的密鑰K_S，該密鑰僅由eNB_1和eNB_2已知。

有這樣一個節點級別強壯密鑰，在I（發起方）和R（回應方）之間的初始交換可以通過以下的消息對600來

保護：

1. $eNB_1 \rightarrow eNB_2$: $HDR_1, SA_1, g_I^X, N_1, \{\underline{HDR_1, SA_1, g_I^X, N_1}\}_{Ks}$

2. $eNB_2 \rightarrow eNB_1$: $HDR_2, SA_2, g_2^y, N_2, \{\underline{HDR_2, SA_2, g_2^y,, N_2}\}_{Ks}$

這些符號對應那些上面所定義的。對於 IPsec 消息 1 和 2，括弧符號標識消息驗證碼（MAC）值被增加，每一個分別代表使用每一消息的所有元件的驗證/完整鑰匙，即，共用秘密 K_S，的散列。每一個使用 K_S 的散列保護其對應的 IPsec 消息。如果，第 6 圖所示的攻擊之後，也就是中間人攻擊，攻擊者嘗試發送 g_I^m 或 g_R^m 到 I，在相應消息中的散列（MAC）將不與由消息的接收方計算的相一致。作為結果，這樣的嘗試，或者任何欺騙嘗試，將被檢測和擊敗。第 7 圖說明了這一關於 X2C 驗證和鑰匙關聯操作的改進的 IPsec 安全關聯。

在第 7 圖中 630 指示的和在第 4 圖中詳述的第二種實施方式，直接 eNB 驗證通過 X2C 被完成。為了保護免受可能的劫持/置換或周圍 eNB 的其他損害，這裏公開了輕量化驗證以確保 eNB 間驗證在節點級別被保證。這與相鄰 eNB 都是被保護的端點的假定相反，如第 4 圖所示，在 LTE 中任何兩對 eNB 之間。

參考第 4 圖，LTE 網路為所有 LTE eNB 準備通用共用密鑰 K 和通用共用 eNB 證書 C 用於 eNB 間驗證。在 eNB 被網路驗證後，自配置 eNB 通過 S1 通道從網路獲取 420

參數。LTE 也使驗證演算法 Fx 和 Fy 標準化，下面進一步描述。

在步驟 400，自配置 eNB 使用鑰匙 K 和安全演算法 Fx 來加密證書 C。結果的加密證書 C’ 被傳輸 410 到相鄰 eNB 並且由相鄰 eNB 使用以驗證自配置 eNB。自配置 eNB 也選擇亂數(RAND)400 並使用 Fx 演算法來從 RAND 400 中計算被加密的驗證值 X-RES。C’ 和 RAND 被傳輸 410 到相鄰 eNB（一個或多個）。

然後，接收的相鄰 eNB（一個或多個）使用 430 共用的密鑰 K 和 Fx 來解碼 C’ 並且將結果與通用 eNB 證書 C 進行比較，該證書已在其記憶體中。同時使用接收到的 RAND 來計算使用 Fy 功能 430 的被解密的驗證值 RES。然後，RES 被往回發送 440 到自配置 eNB 以為其來驗證相鄰 eNB（一個或多個）450。

這一簡化的輕量化 eNB 間驗證避免了 LTE 之前的目前的 UMTS UE 驗證過程中的在 SQN、AK、AMF 和 MAC 上的長度計算，以便減少安全計算負荷，同時通過 X2C 來減少信令消息大小。

同時也有通過 X2C 的 eNB 安全鑰匙關聯 630。假設 IPsec 將被配置以用於 LTE X2 連接，IPsec 的使用和帶有 LTE eNB 提供的安全鑰匙的在“手動”模式的其相關的 IKE-v2，被用僅通過 IPsec 的加密公開。這確保了經由 eNB 通過 LTe 的 X2C 安全和鑰匙的控制，確保了高安全門限。

為了 LTE eNB 受控制的安全鑰匙關聯（用於完整性

保護和加密），提出了下面的選擇：

首先，LTE 可以標準化所有 LTE eNB 中的 X2C 安全保護演算法 Fa。演算法 Fa 可以是目前使用的演算法，如 UMTS f8 或允許資訊的加密和解密的具有共用密鑰的新的演算法，例如 X2C-鑰匙。

第二，LTE 可以通過 X2C 介面標準化安全密鑰的通用集（這可以被選擇以用於 Fa 的最佳安全結果）以用於 eNB 之間的安全應用（完整保護和加密），也就是，所有 LTE eNB 站點已知的一組被索引的 N 個鑰匙可以被定義。

第三，在網路驗證過程之後，如在信令交換“E-UTRAN 參數回應”時間 350，這一用於 LTE X2C 安全操作的通用鑰匙集可以從服務 aGW 下載到自配置 eNB。當 eNB 在預操作模式時，下載到每一個 LTE eNB 的安全鑰匙集可以在 eNB 自配置階段發生，並且因此能夠提供信令負荷處理。現有的操作的 eNB 已經具有保存的鑰匙集。

第四，如果存在一個用於完整保護並且另一個用於解密，則一個或多個安全鑰匙可以在自配置階段、關聯階段或在稍後的用於重新關聯的操作階段通過 X2C 介面被單獨地選擇或在兩個 eNB 對之間被關聯。在關聯階段，只有鑰匙索引需要被相互確定來啟動所同意的單一安全鑰匙的使用。這一過程通過不在消息交換中發送安全鑰匙的根值而使被增加的安全門限有利，如現有技術，通過直接導出安全鑰匙而減少計算負荷以及在鑰匙協定消息交換

中減少信令大小。

第五，在鑰匙協定步驟中，對於相同的一組 X2C-鑰匙的 N 個號碼，Diffie-Hellman 鑰匙索引方法可以被用於交互作用地達到相同的鑰匙索引 I，以便安全鑰匙 X2C-鑰匙[i]將被用於意指的完整保護和/或加密操作。這在第 5 圖中顯示。

第六，導出的安全鑰匙可以被用於完整保護和加密兩者。可替換地，對每一操作期望不同的安全鑰匙。在那種情況下，一種選擇是單獨地以串列或並行的方式對其他的鑰匙操作相同的鑰匙索引交換過程。可替換的選擇是將偏移號碼添加到已經獲取的鑰匙索引，並隨後又採取模 N 操作以達到新的索引[0, N-1]。偏移可以通過使用僅兩個站點已知的號碼而被獲得，例如自配置 eNB-Id 之類的標識號碼。

所有的選擇（和其他的在本發明的範圍內選擇）也可以週期性地操作，即使當 eNB 處於可操作模式中時，以便重新選擇（重新關聯）安全鑰匙。這將減少在長持續攻擊嘗試下被破壞的安全的可能性。

eNB 間驗證和在自配置 eNB 和其相鄰 eNB 之間的安全鑰匙關聯可以被一起結合以達到 eNB 間驗證和在一次交換中的安全關聯兩方面，如第 7 圖所示，該圖說明瞭關於被連接的相鄰 eNB 的通過 X2C 的總體的自配置 eNB 操作。

第 7 圖中的 eNB 間操作看似是點到點操作，但是，

從 eNB 方面來看，它是點到多點操作。因此，如果基本的 IP 層支援這樣的操作，則組播可以由自配置 eNB 使用。但是每一個相鄰 eNB 必須單獨地響應於自配置 eNB。

注意到在第 7 圖中，X2C 同步交換 620 是可選的，如上面關於第 3 圖的描述。同時，在 eNB 間的驗證和安全鑰匙協議 600 中的 Alt-1 是在上面所描述的，其中前兩個 IPsec_Init_SA 消息是被完整性保護的。剩下的 IPsec 步驟隨後可以如 IPsec 正常需要一樣被執行。

如果驗證或鑰匙交換失敗，並且失敗決定是基於幾個連續失敗的嘗試，自配置 eNB 應該考慮 X2C 介面無效並且報告給網路。

接下來的 E-UTRAN（eNB）參數可以從相鄰 eNB 參數交換操作 610 獲取：GPS 定位資訊；eNB 操作的胞元數量和胞元-Id；服務運營商的標識或本地 PLMN Id；eNB 測量或測量組/關聯資訊；用於胞元的無線電參數，如頻段和中心頻率、胞元傳輸帶寬值、功率控制資訊、基線胞元公共通道配置、MIMO 和方向性天線資訊、MBMS SFN 資訊及 MBMS 資源資訊；以及用於胞元的服務參數，如 MBMS 資訊、LCS 資訊和在 eNB 間共用的公共 SI 資訊。

實施例

1．一種用於第一無線基地台的操作的方法。

2．根據實施例 1 所述的方法，其中第一基地台是自配置的。

3．根據實施例 1 或 2 所述的方法，該方法包括使得第一基地台和第二基地台之間交互作用。

4．根據實施例 3 所述的方法，其中第二基地台是第一基地台的相鄰基地台。

5．根據任一前述實施例所述的方法，該方法包括驗證第一和第二基地台。

6．根據實施例 5 所述的方法，所述驗證包括：

第一基地台將參數請求信號傳送到存取閘道；

所述存取閘道接收該參數請求信號並將參數回應信號傳送到第一基地台；

第一基地台用鑰匙編碼第一證書以創建第二證書；

第一基地台生成亂數；

第一基地台使用亂數來生成加密的驗證值；

第一基地台將授權請求傳送到第二基地台；

第二基地台用鑰匙解碼第二證書；

第二基地台使用亂數來生成解密的驗證值；

第二基地台將第二證書與第一證書進行比較；

第二基地台將授權回應傳送到第一基地台；以及

第一基地台加密的和解密的驗證值進行比較。

7．根據實施例 5 或 6 所述的方法，其中所述參數請求信號包括第二基地台資訊。

8．根據實施例 5-7 中任一實施例所述的方法，其中所述參數回應信號包括第一證書、鑰匙和編碼資訊。

9、根據實施例 5-8 中任一實施例所述的方法，其中

所述授權請求信號包括第二證書和亂數。

10．根據實施例 5-9 中任一實施例所述的方法，其中所述授權回應信號包括被解密的驗證值。

11．根據實施例 5-10 中任一實施例所述的方法，該方法還包括第一基地台：

從存取閘道接收 IP 位址；

用存取閘道執行網路驗證；

加電並開啟站間介面；以及

從第二基地台接收標識資訊。

12．根據實施例 5-11 中任一實施例所述的方法，該方法還包括：第一基地台和第二基地台傳送和接收與網際協議安全（IPsec）過程相適應的資訊。

13．根據實施例 5-12 中任一實施例所述的方法，其中所述鑰匙是由整個無線通信系統使用的共用鑰匙。

14．根據實施例 5-13 中任一實施例所述的方法，其中第一證書是在整個無線通信系統上使用的通用證書。

15．根據實施例 12-14 所述的方法，該方法還包括在 IPsec 中建立安全關聯（SA）。

16．根據實施例 15 所述的方法，其中所述 SA 包括安全演算法的說明、IP 目的地地址和用於驗證標頭（AH）或封裝安全有效載荷（ESP）。

17．根據實施例 16 所述的方法，其中所述 AH 或 ESP 包含散列以保護資料的完整性。

18．根據實施例 5-17 中任一實施例所述的方法，包

括使用 Diffie-Hellman 演算法生成用於驗證的第一密鑰和用於加密的第二密鑰。

19．根據實施例 5-18 中任一實施例所述的方法，該方法還包括所述網路準備通用的共用密鑰和用於所有基地台的通用的共用基地台證書以用於站間驗證，其中在相鄰基地台被網路驗證後，第一基地台從相鄰基地台獲取參數。

20．根據實施例 19 所述的方法，其中所述證書由第一基地台加密並且被傳送到相鄰基地台以用於驗證第一基地台。

21．根據實施例 20 所述的方法，該方法還包括相鄰基地台解碼所述證書並且將該證書與通用基地台證書進行比較。

22．根據實施例 5-21 中任一實施例所述的方法，其中第一基地台使用組播信號來與第二基地台通信。

23．一種基地台，該基地台被配置成執行如實施例 1-22 中任一實施例所述的方法。

24．一種用於驗證在第一無線基地台和第二無線基地台之間的通信的方法，該方法包括：

第一基地台和第二基地台從存取閘道接收多個鑰匙；

第一基地台選擇多個鑰匙中的第一個；

第一基地台使用多個鑰匙中的第一個計算第一個值；

第一基地台將第一個值傳送到第二基地台；

第二基地台選擇多個鑰匙中的第二個；

第二基地台使用多個鑰匙中的第二個計算第二個值；

第二基地台使用第一個值和第二個值來計算第一鑰匙索引；

第二基地台將鑰匙關聯回應傳送到第一基地台；以及

第一基地台使用第一個值和第二個值來計算第二鑰匙索引。

25．一種用於無線通信的第一基地台，該基地台包括：

傳輸機，該傳輸機用於將參數請求信號傳送到存取閘道和用於將授權請求傳輸到第二基地台；

接收機，該接收機用於從存取閘道接收參數回應信號和從第二基地台接收授權回應；

編碼器，該編碼器用於使用鑰匙來編碼證書；

亂數生成器，該亂數生成器用於生成亂數；以及

比較器，該比較器用於將被解碼的驗證值和被編碼的驗證值進行比較。

26．根據實施例 25 所述的第一基地台，該基地台被配置成使用亂數來生成被編碼的驗證值。

27．根據實施例 25 或 26 所述的第一基地台，其中所述驗證請求包括被編碼的證書和亂數。

28．根據實施例 25-27 中任一實施例所述的第一基地台，其中所述驗證回應包括被解碼的驗證值。

29．根據實施例 25-28 中任一實施例所述的第二基地台，該基地台還包括：

解碼器，該解碼器用於使用所述鑰匙來解碼被編碼的證

書；

生成器，該生成器用於使用亂數來生成被解碼的驗證值；以及

比較器，該比較器用於將被編碼的證書和所述證書進行比較。

30．一種無線通信系統，該系統包括第一基地台和第二基地台，第一基地台包括：

接收機，該接收機用於從存取閘道接收一組被編入索引的鑰匙；

密鑰導出單元，該密鑰導出單元用於根據該組被編入索引的鑰匙來導出密鑰；以及

傳輸機，該傳輸機用於將鑰匙關聯請求傳送到第二基地台；

接收機，該接收機用於從第二基地台接收鑰匙關聯回應。

雖然本發明的特徵和元素在較佳的實施方式中以特定的結合進行了描述，但每個特徵或元素可以在沒有所述較佳實施方式的其他特徵和元素的情況下單獨使用，或在與或不與本發明的其他特徵和元素結合的各種情況下使用。本發明提供的方法或流程圖可以在由通用電腦或處理器執行的電腦程式、軟體或韌體中實施，其中所述電腦程式、軟體或韌體是以有形的方式包含在電腦可讀存儲介質中的。關於電腦可讀存儲介質的實例包括唯讀記憶體（ROM）、隨機存取記憶體（RAM）、暫存器、快取記憶體、半導體存儲設備、內部硬碟和可移動磁片之類的磁介

質、磁光介質以及 CD-ROM 碟片和數位多功能光碟（DVD）之類的光介質。

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

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

送件申請修正之日期：103 年 10 月 1 日

【圖式簡單說明】

第 1 圖是現有的無線通信系統的方塊圖；

第 2 圖是現有的 LTE 架構的說明；

第 3 圖是本發明公開的方法的一種實施方式的流程圖；

第 4 圖是本發明公開的方法的第二種實施方式的流程圖；

第 5 圖是本發明公開的方法的第三種實施方式的流程圖；

第 6 圖顯示了安全漏洞的已知類型；

第 7 圖是本發明公開的方法的第四種實施方式的流程圖。

【主要元件符號說明】

100、220、EPC	核心網
110	UTRAN
120、RNS	無線電網路系統
130、RNC	無線電網路控制器
135	Node B
140、Iub	鏈路
200、205、eNB	演進型 Node B
210	E-UTRAN
230	S1
240	X2
I	發起方
R	回應方
A	攻擊方

送件申請修正之日期：103 年 10 月 1 日

103年10月01日修正替換頁

十、申請專利範圍：

1. 一種用於無線通信中的一基地台的操作的方法，該方法包括：

將所述基地台加電；

獲取用於所述基地台的一唯一的 IP 地址；

執行一網路驗證；

將一站間介面初始化；

通過所述介面開啟站間同步；

傳輸對網路參數的一請求；以及

接收網路參數使得能夠與一核心網交互作用。

2. 如申請專利範圍第 1 項所述的方法，該方法還包括：

通過所述站間介面獲取關於一鄰近基地台的資訊；

傳輸包含所述資訊的一參數請求；以及

回應於所述請求來接收參數而能夠與所述鄰近基地台交互作用。

3. 如申請專利範圍第 2 項所述的方法，其中關於所述鄰近基地台的該資訊為以下中的至少一者：一基地台識別符、一胞元識別符、公共陸地移動網路識別符和當前操作狀態。

4. 如申請專利範圍第 2 項所述的方法，其中獲取關於該鄰近基地台的資訊包括一同步交換或成對的請求和回應消息。

5. 如申請專利範圍第 1 項所述的方法，該方法還包括接收安全參數用於以下中的至少一者：

送件申請修正之日期：103 年 10 月 1 日

103年10月1日修正替換頁

驗證所傳輸和所接收的消息；以及

通過所述站間介面執行安全密鑰協定過程。

6．如申請專利範圍第 5 項所述的方法，其中所述安全參數包括一通用證書、一通用共用密鑰、一安全演算法和一通用安全鑰匙集中的至少一者。

7．如申請專利範圍第 1 項所述的方法，該方法還包括到達基地台和來自基地台的安全通信，所述安全通信包括：

獲取由所述基地台和一相鄰基地台共用的一密鑰；

傳輸包含第一標頭資訊、一第一安全關聯、一第一鑰匙生成值和一第一現時的散列的一第一消息，所述散列使用所述密鑰；以及

接收包含一第二標頭資訊、一第二安全關聯、一第二鑰匙生成值和一第二現時的散列的一第二消息，所述散列使用所述密鑰。

8．如申請專利範圍第 7 項所述的方法，其中所述第一和第二鑰匙生成值為 Diffie-Helman 參數，該參數用於產生用來生成完整性鑰匙和機密性鑰匙中的至少一者的一種子。

9．如申請專利範圍第 1 項所述的方法，包括通過所述站間介面來執行直接的基地台驗證。

10．如申請專利範圍第 9 項所述的方法，其中所述驗證包括：

接收在基地台之中共用的密鑰；

送件申請修正之日期：103 年 10 月 1 日

接收在基地台之中共用的一證書；

接收共用的多個驗證演算法；

使用所述密鑰和來自所述驗證演算法的一第一演算法來加密所述證書；

選擇一亂數並且使用所述第一演算法從該亂數中生成被一加密的驗證值；

傳送被加密的證書、該亂數和被加密的驗證值；

接收一被解密的驗證值；以及

將所述被解密的和所述被加密的驗證值進行比較。

11．如申請專利範圍第 10 項所述的方法，其中所述被解密的驗證值是使用所述亂數和來自所述驗證演算法的一第二演算法計算出的。

12．如申請專利範圍第 1 項所述的方法，該方法還包括用於完整性保護和加密的受控制的安全鑰匙的關聯，其包括以下的至少一者：

標準化用於所有基地台的一站間安全保護演算法，以允許用一共用安全鑰匙進行加密和解密；以及

標準化對於所有基地台已知的被編入索引的安全鑰匙組。

13．如申請專利範圍第 12 項所述的方法，該方法還包括在網路驗證之後於該基地台接收所述被編入索引的安全鑰匙組。

14．如申請專利範圍第 13 項所述的方法，其中接收所述被編入索引的安全鑰匙組在接收網路參數的期間發生。

15．如申請專利範圍第 12 項所述的方法，其中安全鑰匙被單獨地選擇或者通過相互確定鑰匙索引從而與所述基地台及鄰近基地台相關聯。

16．如申請專利範圍第 15 項所述的方法，其中相互確定鑰匙索引包括使用一 Diffie-Helman 方法。

17．如申請專利範圍第 12 項所述的方法，該方法包括使用用於完整性保護的一鑰匙和用於加密的一不同的鑰匙。

18．如申請專利範圍第 17 項所述的方法，其中所述完整性保護鑰匙和加密鑰匙通過為兩個鑰匙分別地操作一單獨的鑰匙索引交換過程而獲取。

19．如申請專利範圍第 17 項所述的方法，其中所述完整性保護鑰匙和加密鑰匙通過一過程被獲取，該過程包括：

獲取所述鑰匙中的一個；

增加一偏移數；以及

執行一模操作以獲取另一個鑰匙。

20．如申請專利範圍第 19 項所述的方法，其中獲取所述偏移數包括使用僅所述基地台和鄰近基地台已知的數。

21．如申請專利範圍第 1 項所述的方法，該方法還包括：

傳送與相鄰基地台相關的參數的請求；以及

接收所述參數以回應所述請求。

22．如申請專利範圍第 21 項所述的方法，其中接收到的參數為以下中的至少一者：GPS 定位資訊；由所述相鄰基地台操作的胞元的數量；所述胞元中的每一個的

Id、服務運營商的標識或本地 PLMN Id；測量中的資訊、測量組、或用於所述鄰近基地台的測量關聯；所述胞元的無線電參數；以及所述胞元的服務參數。

23．如申請專利範圍第 22 項所述的方法，其中所述無線電參數是以下中的至少一者：頻率波段、中心-頻率、胞元傳輸帶寬值、功率控制資訊、基線胞元公共通道配置、MIMO 和方向性天線資訊、MBMS SFN 資訊以及 MBMS 資源資訊。

24．如申請專利範圍第 22 項所述的方法，其中所述服務參數為以下中的至少一者：MBMS 資訊、LCS 資訊和在鄰近基地台之中共用的公共 SI 資訊。

25．一種無線基地台，該無線基地台包含：

一接收機，其被配置以從一核心網獲取一唯一的 IP 地址；

一處理器，其被配置以執行一網路驗證、將一站間介面初始化以及通過所述介面開啟站間同步；以及

一傳輸機，其配置以傳送對網路參數的一請求；

該接收機被配置以接收網路參數使得能夠與所述核心網交互作用。

26．如申請專利範圍第 25 項所述的基地台，其中

該處理器被配置以通過所述站間介面獲取關於一鄰近基地台的資訊；

該傳輸機被配置以傳送包含所述資訊的一參數請求；以及

送件申請修正之日期：103 年 10 月 1 日

103年10月01日修正替換頁

該接收機被配置以接收參數使得能夠與所述鄰近基地台交互作用。

27．如申請專利範圍第 26 項所述的基地台，該處理器被配置以處理接收的安全參數用於以下中的至少一者：

驗證所傳輸和所接收的消息；以及

通過所述站間介面執行安全密鑰協定過程。

28．如申請專利範圍第 25 項所述的基地台，其中

該接收機被配置以獲取由一相鄰基地台共用的一密鑰；

該傳輸機被配置以傳送包含一第一標頭資訊、一第一安全關聯、一第一鑰匙生成值和一第一現時的散列的一第一消息，所述散列使用所述密鑰；以及

該接收機被配置以使用所述密鑰接收包含一第二標頭資訊、一第二安全關聯、一第二鑰匙生成值和一第二現時的散列的一第二消息，所述散列使用所述密鑰。

29．如申請專利範圍第 28 項所述的基地台，其中所述第一和第二鑰匙生成值為 Diffie-Helman 參數，該參數用於產生用來生成完整性鑰匙和機密性鑰匙中的至少一者的種子。

30．如申請專利範圍第 25 項所述的基地台，其中

該接收機被配置以接收在基地台之中共用的密鑰、接收在基地台之中共用的證書以及接收共用的多個驗證演算法；

該處理器被配置以使用所述密鑰和來自所述驗證演算法的一第一演算法來加密所述證書、選擇一亂數並且使用所述第一演算法從該亂數中生成一被加密的驗證值；

該傳輸機被配置以傳送被加密的證書、亂數和被加密的驗證值；

該接收機更被配置以接收被解密的驗證值；以及

該處理器被配置以將所述被解密的和所述被加密的驗證值進行比較。

31．如申請專利範圍第 30 項所述的基地台，該處理器被配置以當所述被解密的驗證值使用所述亂數和來自所述驗證演算法的第二演算法計算出時，比較被解密的驗證值。

32．一種基地台，包括：

一處理器，被配置成在所述基地台的加電後立即發起一自配置過程，其中：

所述基地台在所述自配置過程期間被驗證；

所述基地台被配置成在所述自配置過程期間從與所述基地台相關的網路接收一第一組配置參數；以及

所述基地台被配置成在所述自配置過程期間從另一基地台接收一第二組配置參數。

33．如申請專利範圍第 32 項所述的基地台，其中：

所述基地台被配置成從所述網路請求所述第一組配置參數；以及

所述基地台被配置成從所述另一基地台請求所述第二組配置參數。

34．如申請專利範圍第 32 項所述的基地台，其中所述基地台被配置成建立與所述網路的一介面以請求所述第一組配置參數並接收所述第一組配置參數。

35．如申請專利範圍第 34 項所述的基地台，其中所述基地台被配置成使用一網際協議（IP）地址來建立所述介面。

36．如申請專利範圍第 32 項所述的基地台，其中所述第二組配置參數包括由所述另一基地台所操作之胞元的一指示。

37．如申請專利範圍第 36 項所述的基地台，其中所述第二組配置參數還包括從所述另一基地台來的通過單一頻率網路（SFN）之多媒體廣播多撥服務（MBMS）資訊。

38．如申請專利範圍第 37 項所述的基地台，其中從所述另一基地台來的所述通過 SFN 之 MBMS 資訊當作同步交換或成對的請求和回應消息而被接收。

39．一種通過一基地台用於自配置的方法，所述方法包括：

在所述基地台的加電後立即通過所述基地台，發起一自配置過程；

在所述自配置過程期間，驗證所述基地台；

在所述自配置過程期間通過所述基地台從與所述基地台相關的網路，接收一第一組配置參數；以及

送件申請修正之日期：103 年 10 月 1 日

在所述自配置過程期間通過所述基地台從另一基地台，接收一第二組配置參數。

40．如申請專利範圍第 39 項所述的方法，還包括：

通過所述基地台從所述網路，請求所述第一組配置參數；以及

通過所述基地台從所述另一基地台，請求所述第二組配置參數。

41．如申請專利範圍第 39 項所述的方法，還包括：

建立與所述網路的一介面以請求所述第一組配置參數並接收所述第一組配置參數。

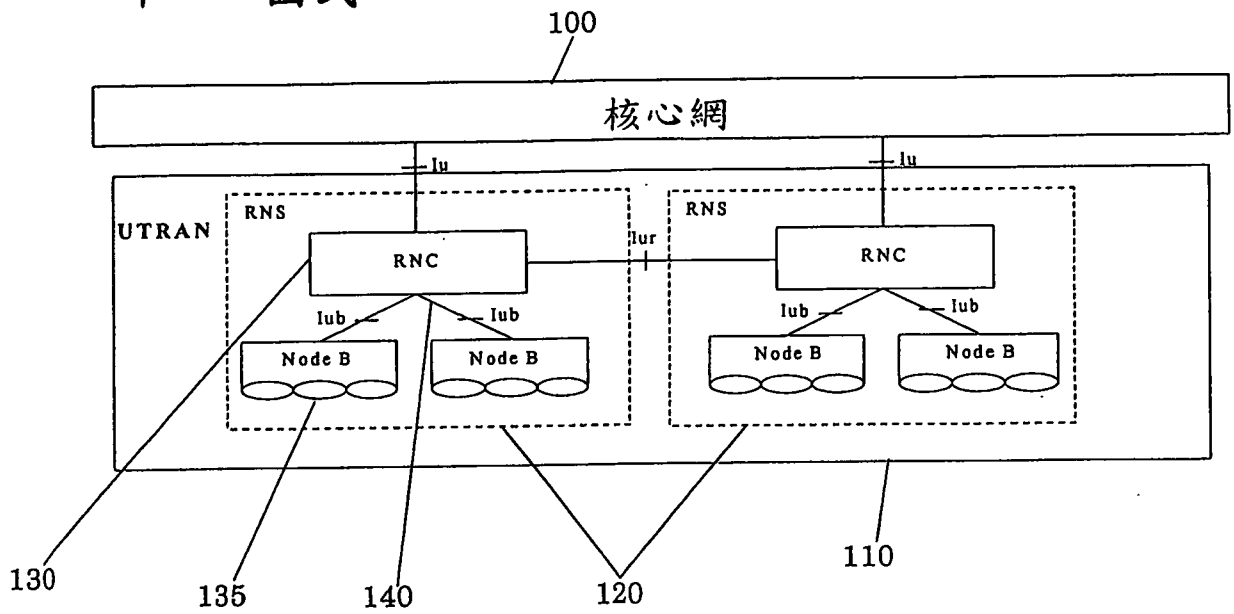
42．如申請專利範圍第 41 項所述的方法，其中所述介面是使用一網際協議（IP）地址而建立。

43．如申請專利範圍第 39 項所述的方法，其中所述第二組配置參數包括由所述另一基地台所操作之胞元的一指示。

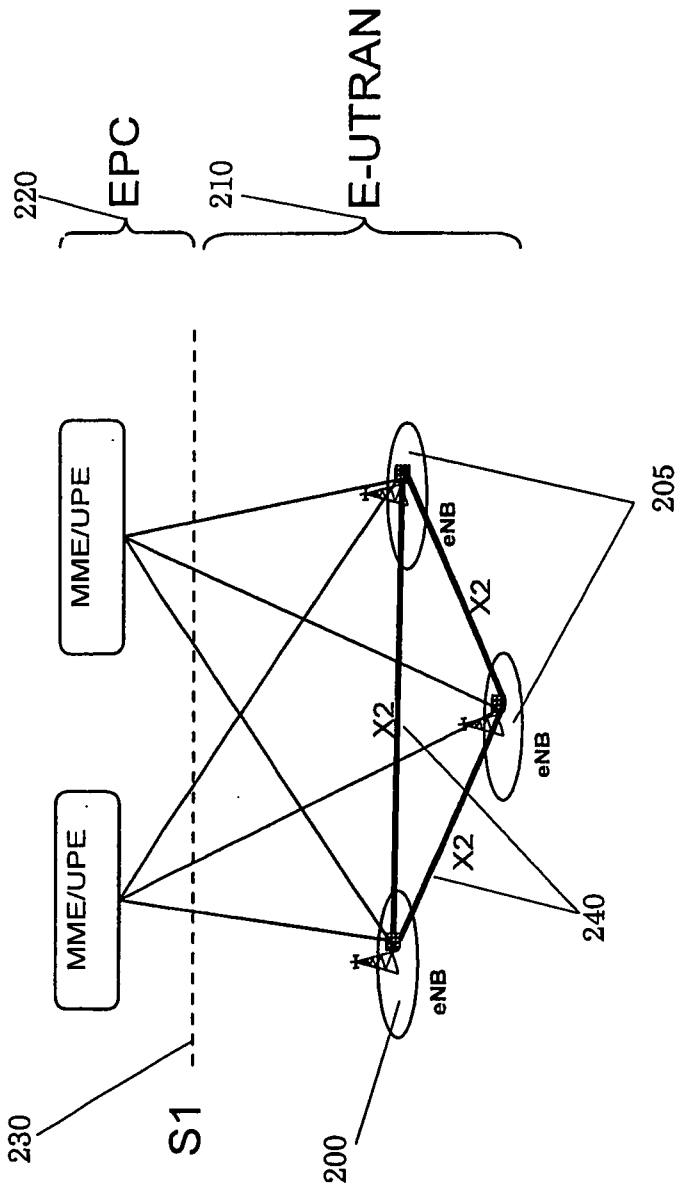
44．如申請專利範圍第 43 項所述的方法，其中所述第二組配置參數還包括從所述另一基地台來的通過單一頻率網路（SFN）之多媒體廣播多撥服務（MBMS）資訊。

45．如申請專利範圍第 44 項所述的方法，其中從所述另一基地台來的所述通過 SFN 之 MBMS 資訊當作同步交換或成對的請求和回應消息而被接收。

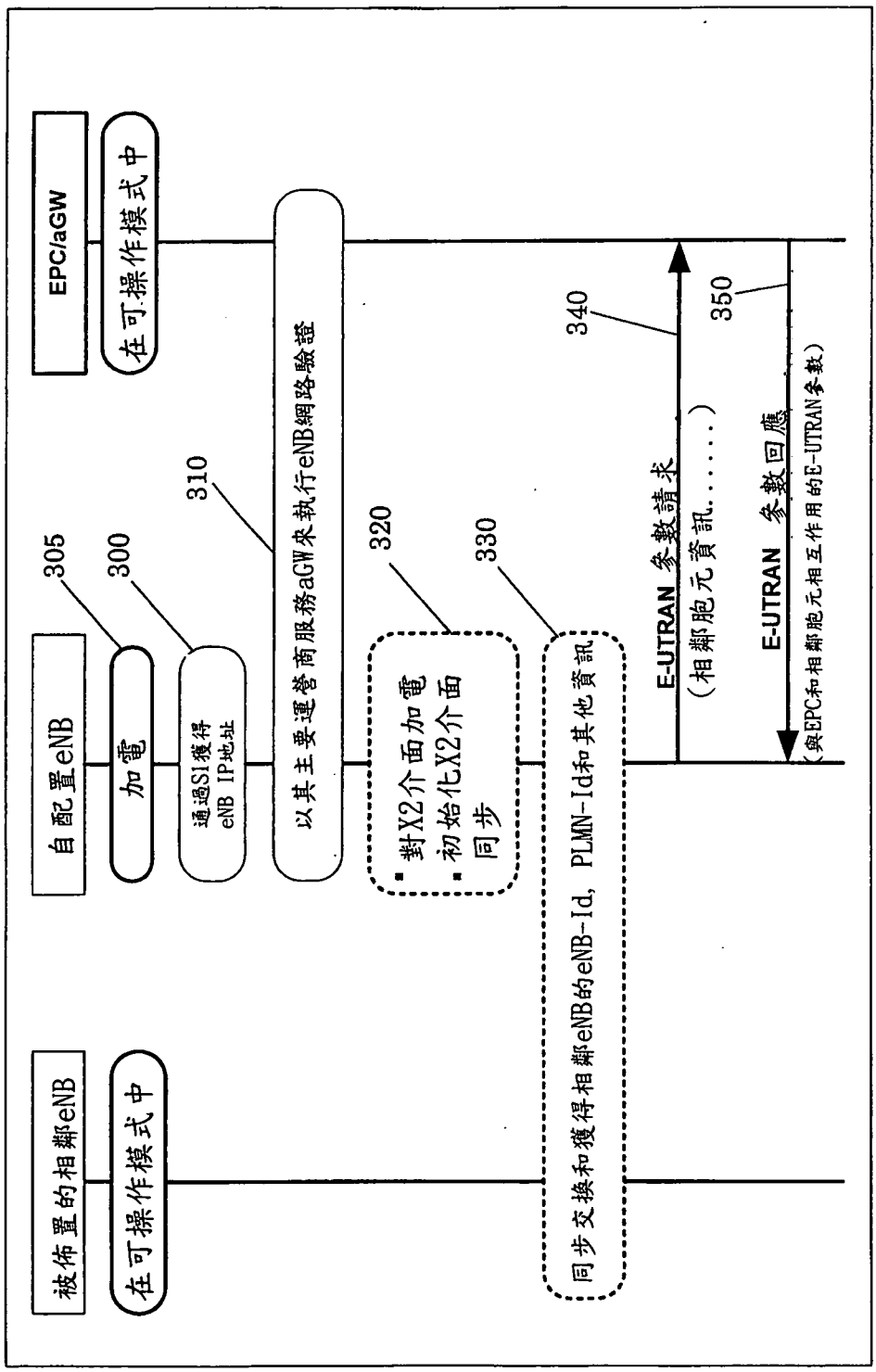
十一、圖式：


100
核心網
Iu
Iu
UTRAN
RNS
RNC
Iur
RNS
RNC
Iub
Iub
Iub
Iub
Node B
Node B
Node B
Node B
130
135
140
120
110

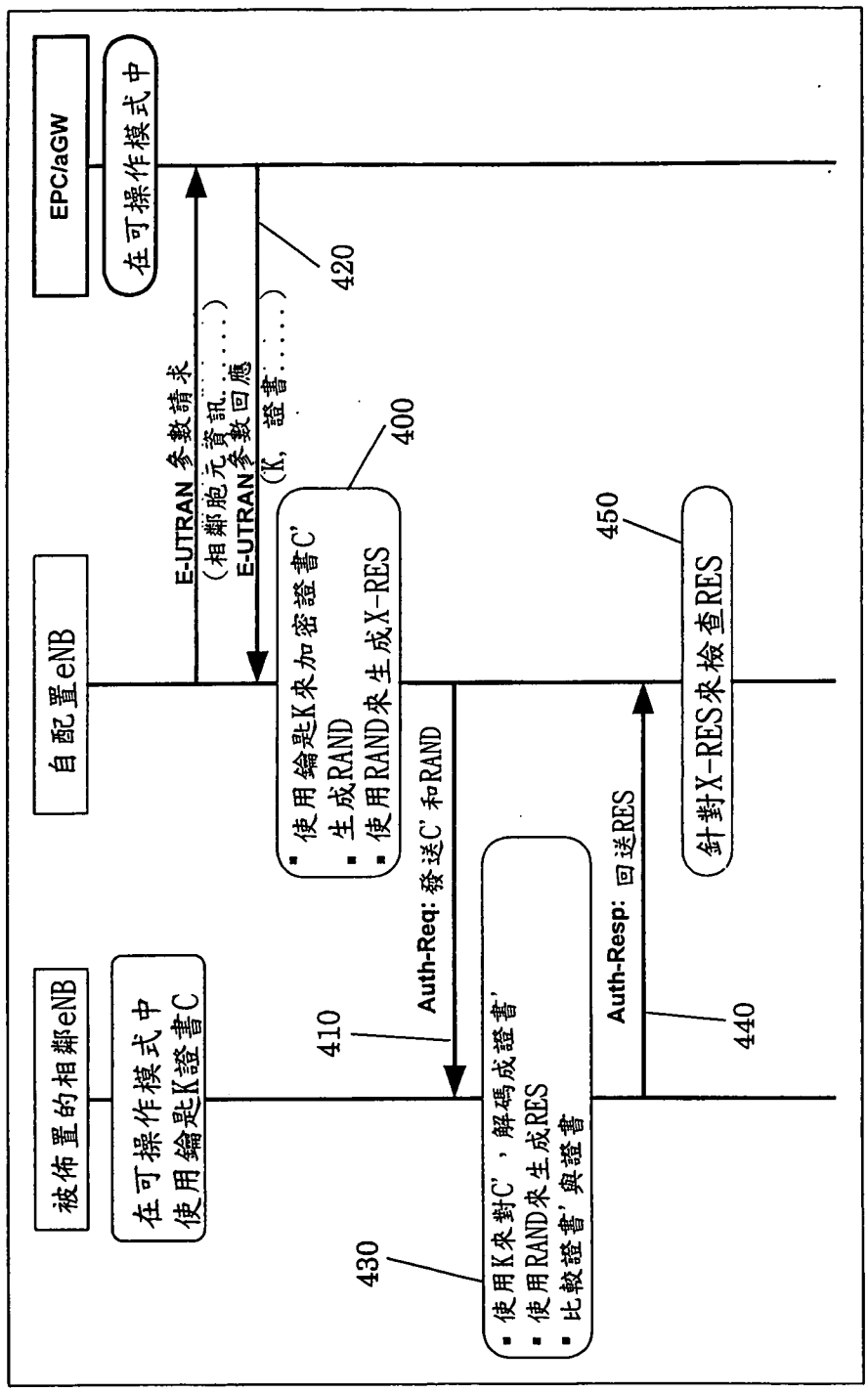
第 1 圖


220
EPC
210
E-UTRAN
MME/UPE
MME/UPE
S1
230
200
eNB
eNB
eNB
X2
X2
X2
205
240

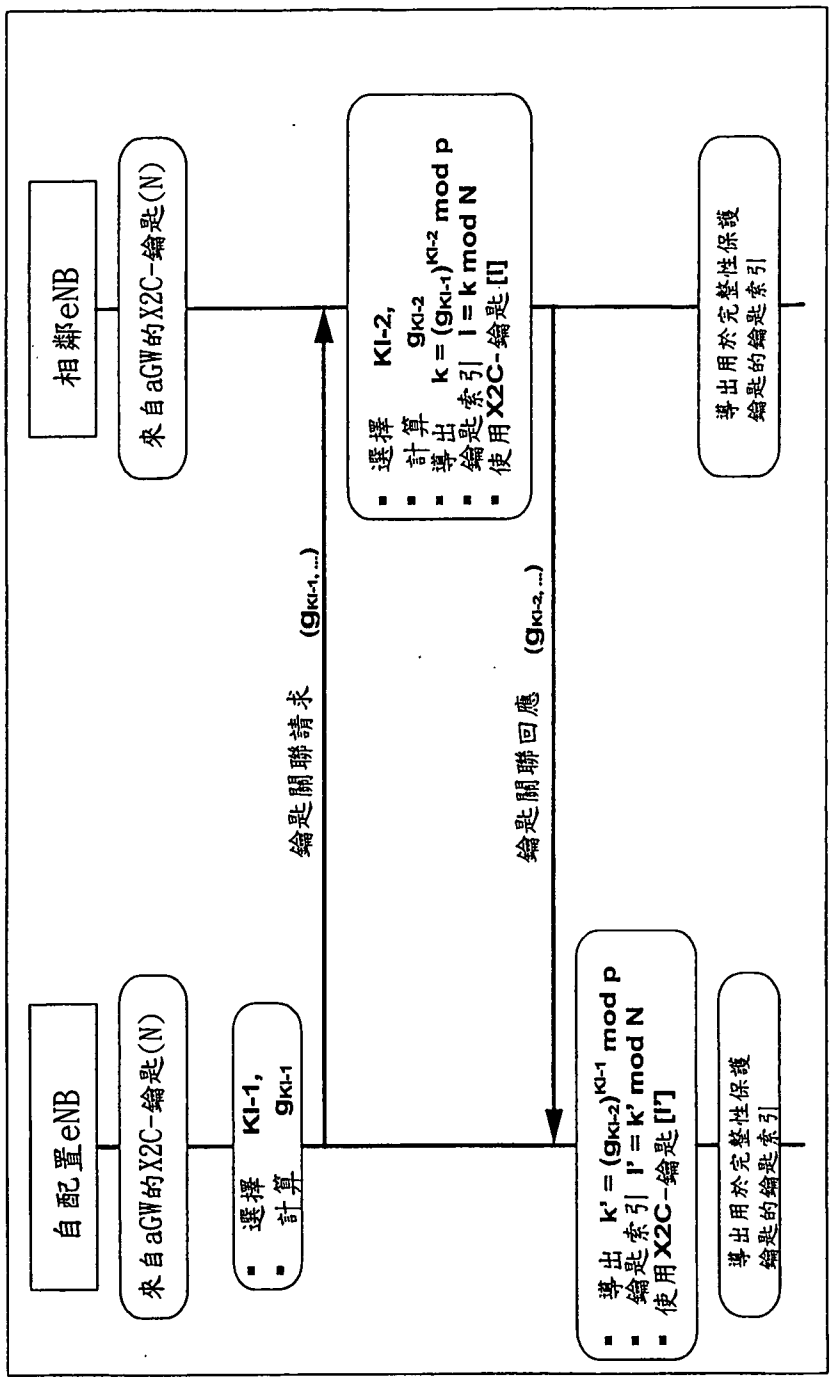
第 2 圖


被佈置的相鄰eNB
在可操作模式中
自配置eNB
305
加電
300
通過S1獲得
eNB IP地址
310
EPC/aGW
在可操作模式中
以其主要運營商服務aGW來執行eNB網路驗證
320
■對X2介面加電
■初始化X2介面
同步
330
同步交換和獲得相鄰eNB的eNB-Id, PLMN-Id和其他資訊
340
E-UTRAN 參數請求
(相鄰胞元資訊.....)
350
E-UTRAN 參數回應
(與EPC和相鄰胞元相互作用的E-UTRAN參數)

第 3 圖


被佈置的相鄰eNB
自配置eNB
EPC/aGW
在可操作模式中
使用鑰匙K證書C
在可操作模式中
E-UTRAN 參數請求
(相鄰胞元資訊.....)
E-UTRAN參數回應
(K, 證書.....)
420
400
使用鑰匙K來加密證書C'
生成RAND
使用RAND來生成X-RES
410
Auth-Req: 發送C' 和RAND
450
針對X-RES來檢查RES
Auth-Resp: 回送RES
440
430
使用K來對C'，解碼成證書'
使用RAND來生成RES
比較證書'與證書

第 4 圖


自配置eNB
來自aGW的X2C-鑰匙(N)
相鄰eNB
來自aGW的X2C-鑰匙(N)
選擇 KI-1,
計算 gKI-1
鑰匙關聯請求 (gKI-1,...)
選擇 KI-2,
計算 gKI-2
導出 k = (gKI-1)KI-2 mod p
鑰匙索引 l = k mod N
使用X2C-鑰匙[l]
導出用於完整性保護鑰匙的鑰匙索引
鑰匙關聯回應 (gKI-2,...)
導出 k' = (gKI-2)KI-1 mod p
鑰匙索引 l' = k' mod N
使用X2C-鑰匙[l']
導出用於完整性保護鑰匙的鑰匙索引

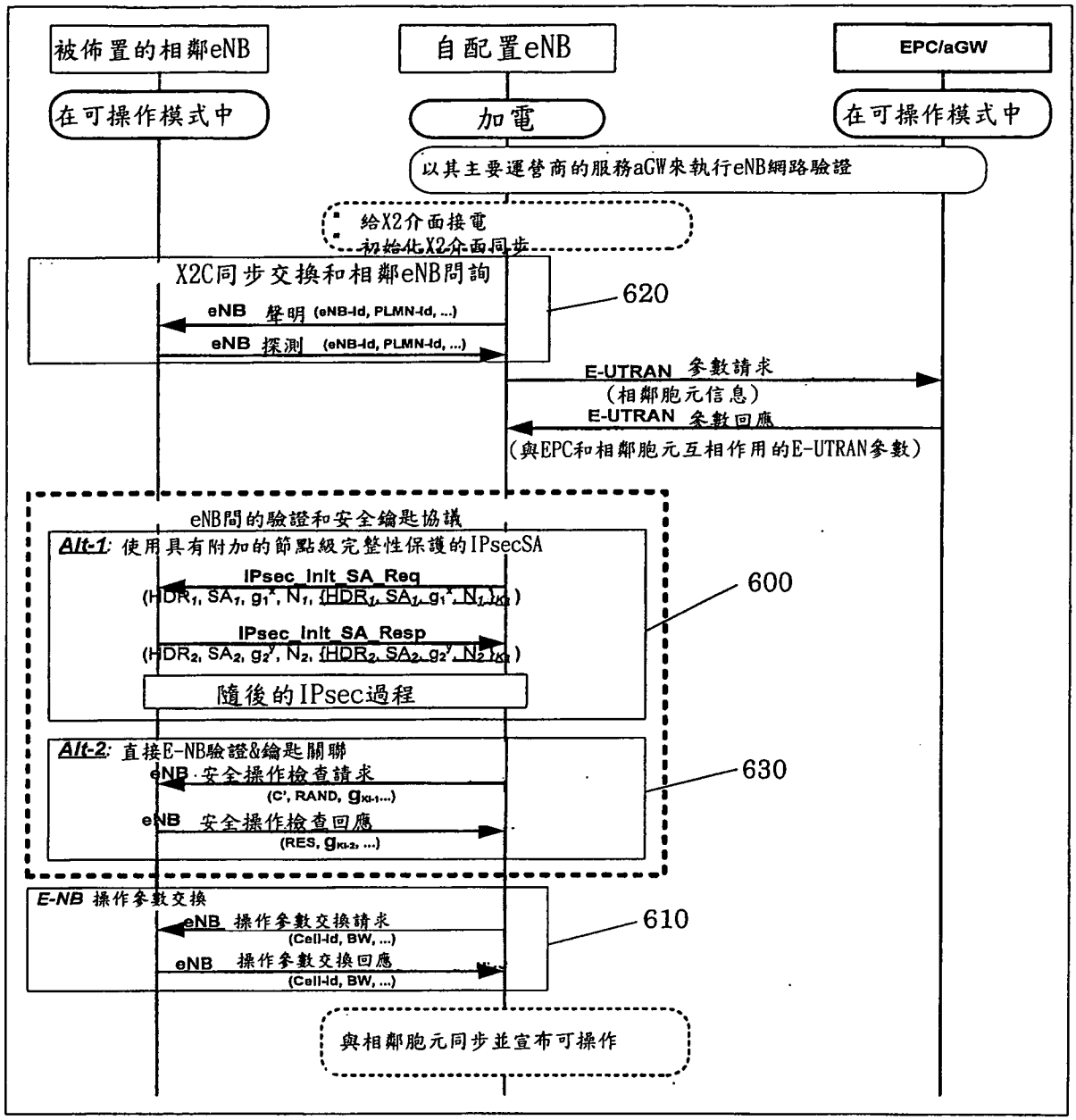
第 5 圖

I: 發起方
R:回應方
A:攻擊方

讓p作為最大的起始號碼並 g 作為乘法群 F_p^* 的生成元
初始地，I挑選x，A挑選m，且R挑選y，所有的整數從間隔〔1, p-1〕中均勻地選擇

1. $I \rightarrow A(R)$: HDR_I, SA_I, g_I^x, N_I (注意：A(R)表示A接收想要用於R的消息)
2. $A(I) \rightarrow R$: HDR_I, SA_I, g_I^m, N_I (注意：A(I)表示來自A的消息，但被接收方假設成是來自I的)
3. $R \rightarrow A(I)$: HDR_R, SA_R, g_R^y, N_R
4. $A(R) \rightarrow I$: HDR_R, SA_R, g_R^m, N_R
5. $I \rightarrow A(R)$: HDR_I, SK{ID_I, $Cert_I$, AUTH, $SA2_I$, ..., 其他欄位以創造子 SAs}
6. $A(I) \rightarrow R$: HDR_I, SK{ID_I, $Cert_I$, AUTH, $SA2_I$, ..., 其他欄位以創造子 SAs}
7. $R \rightarrow A(I)$: HDR_R, SK{ID_R, $Cert_R$, Sig_R, AUTH, $SA2_R$, ..., 其他欄位以創造子 SAs}
8. $A(R) \rightarrow I$: HDR_R, SK{ID_R, $Cert_R$, Sig_R, AUTH, $SA2_R$, ..., 其他欄位以創造子 SAs}

第 6 圖


被佈置的相鄰eNB
自配置eNB
EPC/aGW
在可操作模式中
加電
在可操作模式中
以其主要運營商的服務aGW來執行eNB網路驗證
給X2介面接電
初始化X2介面同步
X2C同步交換和相鄰eNB問詢
620
eNB 聲明 (eNB-Id, PLMN-Id, ...)
eNB 探測 (eNB-Id, PLMN-Id, ...)
E-UTRAN 參數請求
(相鄰胞元信息)
E-UTRAN 參數回應
(與EPC和相鄰胞元互相作用的E-UTRAN參數)
eNB間的驗證和安全鑰匙協議
Alt-1: 使用具有附加的節點級完整性保護的IPsecSA
IPsec_Init_SA_Req
IPsec_Init_SA_Resp
600
隨後的IPsec過程
Alt-2: 直接E-NB驗證&鑰匙關聯
eNB 安全操作檢查請求
(C', RAND, gKi-1...)
eNB 安全操作檢查回應
(RES, gKi-2, ...)
630
E-NB 操作參數交換
eNB 操作參數交換請求
(Cell-Id, BW, ...)
eNB 操作參數交換回應
(Cell-Id, BW, ...)
610
與相鄰胞元同步並宣布可操作

第 7 圖