I474667

(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 I474667 B**

(45)公告日： 中華民國 104 (2015) 年 02 月 21 日

(21)申請案號：101119379 (22)申請日： 中華民國 101 (2012) 年 05 月 30 日

(51)Int. Cl.： *H04L12/22 (2006.01)* *H04L29/10 (2006.01)*

(30)優先權：2011/06/01 美國 61/492,240

2011/06/28 美國 13/170,979

(71)申請人：美國博通公司 (美國) BROADCOM CORPORATION (US)

美國

(72)發明人：克廉 菲利浦 KLEIN, PHILIPPE (IL) ；克里格 艾維 KLIGER, AVI (IL)

(74)代理人：莊志強

(56)參考文獻：

US 6240188B1 US 2008/0130640A1

US 2010/0281249A1

審查人員：謝志偉

申請專利範圍項數：19 項 圖式數：11 共 50 頁

(54)名稱

生成和分佈網路安全參數之系統及方法

NETWORK SECURITY PARAMETER GENERATION AND DISTRIBUTION

(57)摘要

本發明所揭露的各種實施方式有助於在包含多種異構鏈路層聯網技術的聚合式網路內生成和分佈網路安全參數。所提供的實施方式使用聚合式網路密碼通過多種異構鏈路層聯網技術連接網路裝置。所提供的實施方式使用配對事件協定通過多種異構鏈路層聯網技術連接網路裝置，此配對事件協定例如為按鈕協定。

Disclosed are various embodiments for facilitating network security parameter distribution and generation in a converged network incorporating multiple heterogeneous link layer networking technologies. Embodiments are provided for connecting network devices through multiple heterogeneous link layer networking technologies using a converged network password. Embodiments are provided for connecting network devices through multiple heterogeneous link layer networking technologies using a pairing event protocol, such as, for example, a push button protocol.

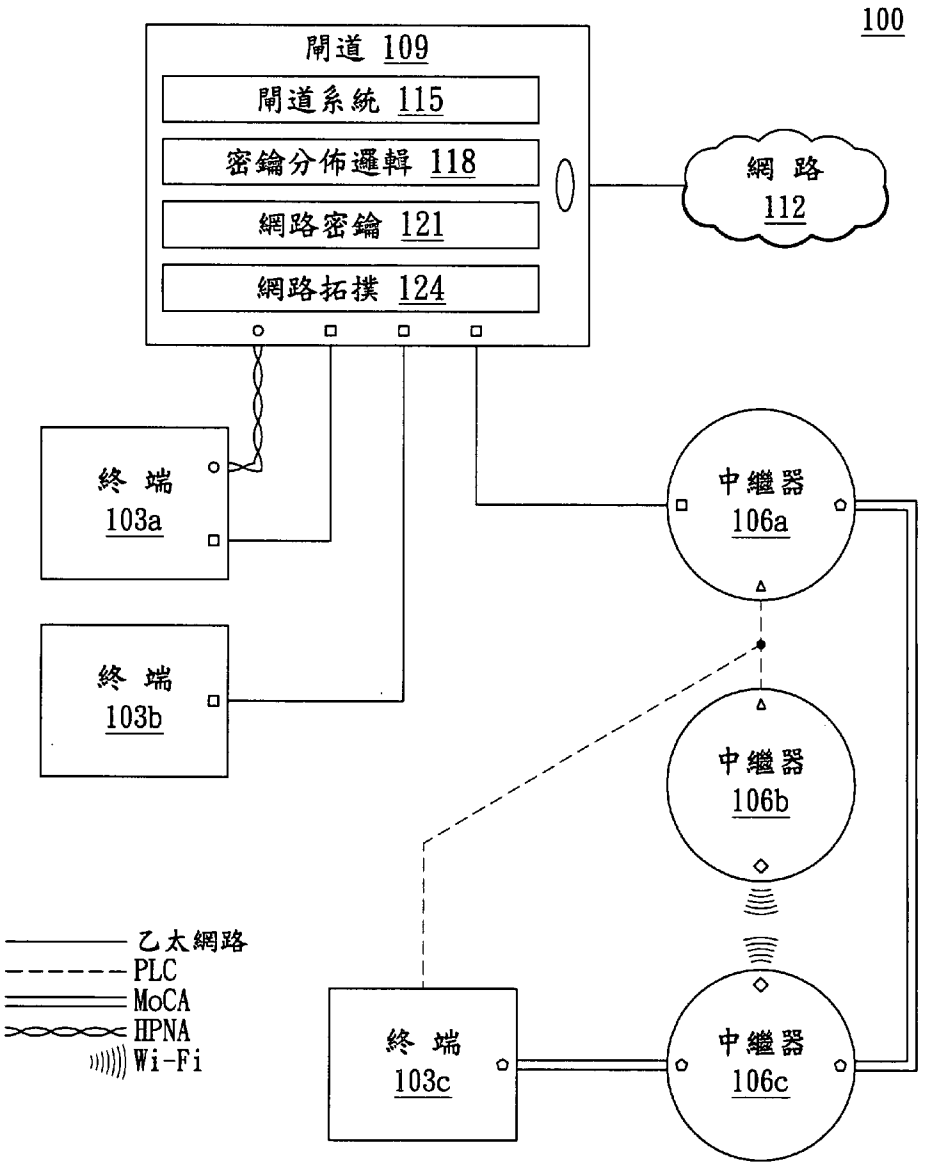

圖1

100・・・聚合式網路

103a、103b、

103c・・・終端

106a、106b、

106c・・・中繼器

112・・・網路

109・・・閘道

115・・・閘道系統

118・・・密鑰分佈邏輯

121・・・網路密鑰

124・・・網路拓撲

發明專利說明書 公告本

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101119379

※申請日：101、5、30 ※IPC分類：H04L 12/52 (2006.01)

H04L 29/10 (2006.01)

一、發明名稱：（中文/英文）

生成和分佈網路安全參數之系統及方法 /

NETWORK SECURITY PARAMETER GENERATION AND DISTRIBUTION

二、中文發明摘要：

本發明所揭露的各種實施方式有助於在包含多種異構鏈路層聯網技術的聚合式網路內生成和分佈網路安全參數。所提供的實施方式使用聚合式網路密碼通過多種異構鏈路層聯網技術連接網路裝置。所提供的實施方式使用配對事件協定通過多種異構鏈路層聯網技術連接網路裝置，此配對事件協定例如為按鈕協定。

三、英文發明摘要：

Disclosed are various embodiments for facilitating network security parameter distribution and generation in a converged network incorporating multiple heterogeneous link layer networking technologies. Embodiments are provided for connecting network devices through multiple heterogeneous link layer networking technologies using a converged network password. Embodiments are provided for connecting network devices through multiple

heterogeneous link layer networking technologies using a pairing event protocol, such as, for example, a push button protocol.

四、指定代表圖：

(一)本案指定代表圖為：圖 1。

(二)本代表圖之元件符號簡單說明：

100：聚合式網路

103a、103b、103c：終端

106a、106b、106c：中繼器

112：網路

109：閘道

115：閘道系統

118：密鑰分佈邏輯

121：網路密鑰

124：網路拓撲

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：

交叉引用相關申請

本申請要求2011年6月1日提交的題為“生成與分佈網路安全參數(NETWORK SECURITY PARAMETER GENERATION AND DISTRIBUTION)”、申請號為61/429,240的美國臨時專利申請的優先權和權益，其全部內容通過引用結合於此。

【發明所屬之技術領域】

本發明有關於一種聚合式網路，且特別是有關於一種具有生成和分佈網路安全參數的聚合式網路。

【先前技術】

家庭聯網中存在多種不同類型的技術。一些家庭具有運行至不同位置的超5類或更好的非遮罩雙絞線(UTP)佈線，在這種類型的電纜上可運行電氣與電子工程師協會(IEEE)802.3乙太網路(Ethernet)。然而，許多家庭可能不能連接到乙太網路，並且添加這種線路可能成本太高。

IEEE 802.11 Wi-Fi為允許進行無線家庭聯網的替代品，但是由於干擾、距離、視線阻礙等等，其性能容易降低。家庭私人網路適配器(HPNA)以及同軸電纜多媒體聯盟(MoCA)分別提供通過普通老式電話服務(POTS)電纜和同軸電纜(這些可能已經存在於電話和/或電視服務房間內)進行聯網的標準。電源線通信(PLC)標準，例如IEEE 1901、HomePlug AV等等，提供通過交流(AC)電源線進行的聯網，在任何電源插座處均可用。由於各種聯網技術的特徵不同，家庭可採用多種技術。

【發明內容】

本發明實施例提供一種系統，此系統包括多個網路裝置，透過採用多種異構鏈路層技術的聚合式資料通信網路進行資料通信。其中，所述網路裝置中的至少一個網路裝置包括到所述聚合式資料通信網路的多個網路介面，所述網路介面中的第一網路介面採用所述異構鏈路層技術中的第一異構鏈路層技術，所述網路介面中的第二網路介面採用所述異構鏈路層技術中的第二異構鏈路層技術。所述網路裝置中的所述至少一個網路裝置進一步地包括網路安全參數管理邏輯，所述網路安全參數管理邏輯被配置為：獲得聚合式網路密碼；以及通過至少部分地基於所述聚合式網路密碼、使用相應的一種異構鏈路層技術的本地配對協定為所述網路介面中的一個網路介面配對，連接至所述聚合式資料通信網路。

【實施方式】

本發明涉及在採用多個異構鏈路層技術的聚合式資料通信網路中生成和分佈網路安全參數。電氣與電子工程師協會（IEEE）P1905.1 為討論中的一個標準，該標準能夠使用多個不同鏈路層聯網技術（例如 IEEE P1901 電源線通信（PLC）、IEEE 802.11 Wi-Fi、IEEE 802.3 乙太網路、同軸電纜多媒體聯盟（MoCA）1.1 和/或其他聯網技術），在家庭網路或其他網路中連接裝置。IEEE P1905.1 限定了抽象層（abstraction layer），該層為異構聯網技術提供通用資料和控制服務接入點，以便提供無縫用戶體驗。由於家庭中網路裝置的位置、網路裝置的性能、應用程式的特定品質服務需要和/或其他原因，可採用不同的聯網技術。

本發明的各種實施方式有助於在IEEE P1905.1網路和/或相似的網路內生成和分佈網路安全參數。在一個實施方式中，用戶可提供單個聚合式網路密碼，用於每個支援的鏈路技術的本地安全/保密協定的各個安全和保密參數可源自該密碼。這種本地協定的實例可包括IEEE P1901簡單連接，Wi-Fi受保護設置（WPS：Wi-Fi Protected Setup）等等。在另一個實例中，可使用利用密鑰分佈的按鈕配對（push-button pairing）將任何網路裝置配對至聚合式資料通信網路。在一時間段內，在新裝置上可按下按鈕並且在聚合式網路上的任何其他裝置上可按下另一按鈕，以有助於配對，即使這兩個裝置不共用相同鏈路層聯網技術的共同鏈路。

術語“配對”此處用於表示將網路裝置認證至通過加密和/或其他安全/保密控制進行保護的聚合式網路。在各種實施方式中，配對交換網路密鑰，而非交換密碼，而且密碼不能源自密鑰。而且，可保持網路分離，使得來自一個聚合式網路的密鑰不被分佈給不同的聚合式網路的裝置。在下面的討論中，大致描述該系統和其部件，然後討論其操作。

請參照圖1，圖1示出了根據各種實施方式的聚合式網路的一個實例的功能方塊圖。聚合式網路100有助於在多個終端103、多個中繼器106、閘道109以及網路112之間進行資料通信。網路112例如包括網際網路、內部網、外部網、廣域網（WAN）、局域網（LAN）、有線網、無線網或者其他合適的網路等，或者兩個以上這種網路的任何組合。雖然圖1中示出了閘道109以及網路112，但是聚合式

網路 100 的其他實例中可能沒有閘道 109 和/或網路 112。

終端 103 和中繼器 106 對應於聚合式網路裝置，可包括任何類型的計算裝置。每個終端 103 和中繼器 106 對應於一個聚合式網路裝置，包括其邏輯鏈路控制（LLC）層和下面的異構鏈路層（媒體存取控制/物理層（MAC/PHY））之間的抽象層。每個終端 103 能夠將聚合式網路管理訊框中繼到其他聚合式網路裝置中。每個中繼器 106 能夠將聚合式網路管理訊框以及資料訊框中繼到其他聚合式網路裝置中。

在圖 1 的實例中，聚合式網路 100 採用五種異構鏈路層技術：乙太網路、PLC、MoCA、電話線上 HomePNA（HPNA）連接以及 Wi-Fi。圖 1 中所示的聯網技術僅構成聚合式網路 100 中可採用的異構聯網技術的一個非限制性實例。使用圖 1 的圖例中的各個標記，在圖 1 中示出了終端 103、中繼器 106 以及閘道 109 之間的連接。利用異構聯網技術中的每種所具有的各自的形狀，在圖 1 中描繪了各聚合式網路介面。方形表示乙太網路介面，三角形表示 PLC 介面，五角形表示 MoCA 介面，圓形表示 HPNA 介面以及菱形表示 Wi-Fi 介面。

閘道 109 可包括閘道系統 115、密鑰分佈邏輯 118 以及其他可執行的應用程式和/或數位邏輯。閘道 109 可存儲資料，例如網路密鑰 121、網路拓撲 124 和/或其他資料。在通常情況下，通過電纜數據機、數位用戶線（DSL）、WiMAX、普通老式電話服務（POTS）撥號、綜合業務數位網（ISDN）、T1、和/或另一種連接，閘道系統 115 為終端 103 和中繼器 106 提供對 WAN 網路 112 的訪問。閘道系統 115 可包括

路由功能、防火牆功能、網路位址轉換（NAT）功能和/或其他功能。

在一個實施方式中，密鑰分佈邏輯 118 為聚合式網路 100 提供集中式密鑰分佈功能。用於聚合式網路 100 的對應於不同的聯網技術的區段或部分的網路密鑰 121 可被保持在閘道 109 中。此外，在閘道 109 中可保持用於聚合式網路 100 的網路拓撲 124，以便密鑰分佈邏輯 118 分佈合適的網路密鑰 121。在另一個實施方式中，可在所有聚合式網路裝置中執行密鑰分佈邏輯 118，以便提供將要描述的分散式密鑰分佈功能。而且，在另一個實施方式中，可從閘道 109 在不同的聚合式網路裝置中執行密鑰分佈邏輯 118，以提供集中式密鑰分佈功能。

請參照圖 2，圖 2 示出了根據本發明的一個實施方式的網路裝置的示意性框圖。網路裝置 200 可對應於於聚合式網路 100（圖 1）中的終端 103（圖 1）或中繼器 106（圖 1）。網路裝置 200 包括至少一個處理器電路，例如具有處理器 203 和記憶體 206，均耦合到本地介面 209。為此，網路裝置 200 例如可包括至少一個通用計算裝置、至少一個嵌入式計算裝置、路由器、交換機和/或可耦合到聚合式網路 100 中的任何其他裝置。可理解，本地介面 209 例如可包括具有伴隨的位址/控制匯流排或其他匯流排結構的一條或多條資料匯流排。

多個網路介面 212a…212N 和一個配對裝置 215 也可耦合到本地介面 209。網路介面 212 對應於聚合式網路 100 的 MAC/PHY 介面，聚合式網路 100 在某些情況下可採用不同的 MAC/PHY 聯網技術。配對裝置 215 可對應於於按鈕配

對裝置、發起配對的通用串列匯流排（USB）電子狗、生物（biometric）配對裝置、基於軟體的虛擬配對裝置和/或任何其他協調系統，以發起到聚合式網路 100 的認證並且與聚合式網路進行配對，而無需手動指定網路密碼。

可由處理器 203 執行的資料和若干元件均儲存在記憶體 206 中。具體地，MAC 抽象層 218、密鑰管理邏輯 221 以及潛在的其他應用程式儲存在記憶體 206 中並且可由處理器 203 執行。網路密鑰 224 和其他資料也可儲存在記憶體 206 中。此外，作業系統可儲存在記憶體 206 中，並且也可由處理器 203 執行。在各種實施方式中，所有或部分 MAC 抽象層 218 和/或密鑰管理邏輯 221 可對應於不單獨由處理器 203 執行的數位邏輯。

執行 MAC 抽象層 218，以便給各種異構聯網技術提供通用資料和控制服務接入點。MAC 抽象層 218 可支援動態介面選擇，用於傳輸來自任何網路介面 212 或上協定層的資料包。MAC 抽象層 218 也可支援端對端服務品質（QoS）。在各種實施方式中可執行密鑰管理邏輯 221，以便生成網路密鑰 224、與其他網路裝置 200 共用網路密鑰 224、從其他網路裝置 200 獲得網路密鑰 224 和/或執行其他功能。

請參照圖 3，圖 3 示出了根據本發明的一個實施方式的閘道的示意性框圖。閘道 109 包括至少一個處理器電路，例如具有處理器 303 和記憶體 306，均耦合到本地介面 309。為此，閘道 109 例如可包括至少一個通用計算裝置、至少一個嵌入式計算裝置、路由器、交換機和/或可耦合至聚合式網路 100（圖 1）的任何其他裝置。可理解，本地介面 309 例如可包括具有伴隨的位址/控制匯流排或其他匯流排

結構的一條或多條資料匯流排。多個網路介面 212a…212N（圖 2）、一個配對裝置 215（圖 2）以及 WAN 介面 312 也可耦合到本地介面 309。WAN 介面 312 用於將閘道 109 連接到網路 112（圖 1）。

可由處理器 303 執行的資料和若干元件均儲存在記憶體 306 中。具體地，閘道系統 115、MAC 抽象層 218、密鑰管理邏輯 221、密鑰分佈邏輯 118 以及潛在的其他應用程式儲存在記憶體 306 並且可由處理器 303 執行。網路拓撲 124、網路密鑰 121 和其他資料也可儲存在記憶體 306 中。此外，作業系統可儲存在記憶體 306 中，並且也可由處理器 303 執行。在各種實施方式中，所有或部分閘道系統 115、MAC 抽象層 218、密鑰管理邏輯 221 和/或密鑰分佈邏輯 118 可對應於不單獨由處理器 303 執行的數位邏輯。

請參照圖 4，圖 4 示出了根據本發明的各種實施方式的表示聚合式網路 100（圖 1）中採用的分層網路模式 400 的示意圖。在分層網路模式 400 中，上層實體 403 將資料傳送給 MAC 抽象層 218，用於發送到聚合式網路 100，並且通過 MAC 抽象層 218 從聚合式網路 100 中獲得資料。根據開放式系統互連（OSI）模式，上層實體 403 可對應於第三層或更高的層。例如，上層實體 403 可對應於互聯網協定（IP）、用戶資料報協定（UDP）、傳輸控制協議（TCP）和/或其他上層實體 403。

MAC 抽象層 218 為上層實體 403 提供與 MAC 無關的單個統一的介面。MAC 抽象層 218 可為網路介面 212（圖 2 和圖 3）提供一個或多個到抽象層的 MAC 專用介面。在圖 4 中，多個 MAC 類型 406a、406b…406N 被示出為結合

多個 PHY 類型 409a、409b…409N。每個 PHY 類型耦合到多個網段 412a、412b…412N 中的各自的一個。網段 412 可分別對應於 Wi-Fi、IEEE 1901、MoCA、乙太網路和/或其他類型的網段 412。從網路裝置 200（圖 1）中的作業系統的觀點來看，MAC 抽象層 218 可被視為輸出資料和控制服務接入點（SAP）的單個裝置。MAC 位址（例如 48 比特位址或某個其他長度）可被分配給 MAC 抽象層 218。MAC 位址對於每個聚合式網路 100 而言可以是唯一的。

現在一併參看圖 1 至圖 4，提供了聚合式網路 100 的各元件的操作的總體描述。首先，假定的家庭設置被用於描述圖 1 的各種元件。例如，假設閘道 109 為小型集成路由器/交換機裝置，位於房屋的底層，靠近網路 112 電路的終端。在該實例中，閘道 109 具有 HomePNA 網路介面 212 以及對應於可橋接或可不橋接的獨立埠的多個乙太網路介面 212。通過 IEEE 802.1AE（MACsec）或另一標準，乙太網路可被保護或者可不被保護。通過 Wi-Fi 保護接入 2（WPA2）或另一標準，Wi-Fi 網路可被保護。

例如，假設終端 103a 為膝上型電腦，有時可靠近家庭中乙太網路埠或電話插座。通過到閘道 109 的 HomePNA 網路介面 212 和/或通過到閘道 109 的乙太網路介面 212，將終端 103a 連接到聚合式網路 100。例如，假設終端 103b 為臺式電腦，該電腦也物理上位於家庭的底層。通過到閘道 109 的乙太網路介面 212，將終端 103b 連接到聚合式網路 100。

例如，假設中繼器 106a 為底層中的裝置，被配置成通過乙太網路介面 212 在閘道 109 之間中繼網路流量以及通

過 PLC 網路介面 212 和 MoCA 網路介面 212 將網路流量中繼到其他網路裝置 200。因此，通過房屋的其他房間中現有的同軸電纜和/或電源線，這些裝置可連接到聚合式網路 100，無需使用 Cat5e 或其他電纜佈線。例如，假設中繼器 106b 位於家庭的主要樓層，並且被用於將 Wi-Fi 網路上的潛在裝置連接到聚合式網路 100。為此，中繼器 106b 可包括 PLC 網路介面 212 和 Wi-Fi 網路介面 212。

例如，假設中繼器 106c 為機頂盒，具有兩個 MoCA 網路介面 212 和一個 Wi-Fi 網路介面 212。假設中繼器 106c 位於具有同軸電纜插座的家庭的較高樓層的臥室中。中繼器 106c 可通過 Wi-Fi 連接到中繼器 106b，以及通過 MoCA 連接到中繼器 106a。例如，假設終端 103c 為數位電視，也位於較高層的臥室中。假設終端 103c 的 MoCA 網路介面 212 通過同軸電纜連接到中繼器 106c，並且終端 103c 的 PLC 網路介面 212 通過家庭的電源線連接到中繼器 106a 和中繼器 106b。

除了連接具有不同聯網技術的網路介面 212 的網路裝置 200，在圖 1 中可看出，在聚合式網路 100 中可提供冗餘路徑。這種冗餘路徑可由 MAC 抽象層 218 進行平衡，以增大網路裝置 200 之間的吞吐量。作為非限制性實例，終端 103a 和閘道 109 之間的 HomePNA 鏈路可提供 20 百萬位元每秒的資料率，同時終端 103a 和閘道 109 之間的 10-Base-T 鏈路可提供 10 百萬位元每秒的資料率。MAC 抽象層 218 可被配置成對鏈路進行組合，以在終端 103a 和閘道 109 之間提供高達 30 百萬位元每秒的總數據率。

而且，當一個鏈路的連接性減弱或丟失時，聚合式網

路 100 的冗余路徑可用於提供可靠的連接。作為非限制性實例，在家庭中操作電力裝置時，PLC 連接容易受到脈衝噪音和/或其他干擾的影響。因此，當終端 103c 和中繼器 106a 之間的 PLC 鏈路減弱、超載、不可使用等時，可代替 PLC 鏈路而在兩個 MoCA 鏈路上路由終端 103c 和中繼器 106a 之間的網路流量。

通過用戶密碼配置或按鈕配置方法，可將網路裝置 200 配對至聚合式網路 100。在用戶密碼配置中，用戶為每個網路裝置 200 手動提供相同的聚合式網路密碼。每個所支援的鏈路層技術的本地安全/保密協定的單個安全/保密參數（例如網路密鑰 224）源自這一單個聚合式網路密碼。作為非限制性實例，可採用散列（hash）函數為每個所支援的鏈路層技術生成單個密碼。作為另一個非限制性實例，可採用散列函數生成任何一個鏈路層技術所需要的最大密碼尺寸，並且可將該密碼縮短（截短），以便為其他鏈路層技術創建較小的密碼。一旦鏈路層密碼源自聚合式網路密碼，那麼每個網路介面 212 執行其自身的本地安全協議並且可獲得額外的安全參數。

利用按鈕配置方法，每當通過配對裝置 215 在網路裝置 200 中發生配對事件時，網路裝置 200 廣播配對事件，以將聚合式網路 100 通知給其他網路裝置 200。一旦獲得配對事件，網路裝置 200 在每個其所支援的網路介面 212 上發起本地按鈕配對協定。網路裝置 200 通過本地按鈕配對協定進行配對。如果通過多個鏈路類型連接新的網路裝置 200，那麼執行每個鏈路的本地按鈕配對協定，以獲得每個鏈路類型的共用網路密鑰 224。網路密鑰 224 可通過集中式

密鑰分佈方法或分散式密鑰分佈方法來分佈。

要注意的是，可物理上或邏輯上驅動配對裝置 215。即，可按壓網路裝置 200 上的物理按鈕，或者可通過軟體來驅動邏輯配對裝置 215。而且，可使用除按鈕外的其他類型的配對裝置 215，例如 USB 電子狗、生物掃描器等等。

在某些情況下，在同一聚合式網路 100 內可結合基於密碼的配對使用按鈕配對。在第一種情況下，假設兩個網路裝置 D1 和 D2 通過本地配對事件協議進行配對，並且生成 Key1A。假設網路裝置 D3 僅支援一個用戶密碼。在配對 D3 之前，用戶在 D1（或 D2）上輸入密碼。D1 從用戶密碼中獲得 Key2A、Key2B 以及 Key2C。D1 將 Key2A、Key2B 以及 Key2C 廣播給 D2。Key2A、Key2B 以及 Key2C 可重寫先前的任何密鑰，例如 Key1A。用戶輸入密碼之後，D3 被配對至聚合式網路。D3 從用戶密碼中獲得相同的 Key2A、Key2B 以及 Key2C。假設網路裝置 D4 支援本地配對事件協定，但不支援基於密碼的配對。D4 通過本地配對事件協議獲得 Key2A、Key2B 和/或 Key2C。

在第二種情況下，假設用戶在網路裝置 D1 和 D2 中輸入密碼。D1 和 D2 從用戶密碼中獲得 Key2A、Key2B 以及 Key2C。假設網路裝置 D3 支援本地配對事件協定，而不支援基於密碼的配對。如果 D1 或 D2 支援本地配對事件協議，那麼 D3 可通過該本地配對事件協議從 D1 或 D2 中獲得 Key2A、Key2B 和/或 Key2C。接下來結合圖 5 至圖 11，進一步討論聚合式網路 100 中的配對。

請參照圖 5，圖 5 示出了提供根據各種實施方式的密鑰管理邏輯 221（圖 2）的一部分的操作的一個實例的流程圖

。具體地，圖 5 涉及使用用戶密碼配置在聚合式網路 100（圖 1）中提供配對的實施方式。應理解，圖 5 的流程圖提供可用於實施文中所述的密鑰管理邏輯 221 的一部分的操作的多種不同類型的功能配置的僅僅一個實例。另外，圖 5 的流程圖可被視為描述根據一個或多個實施方式的網路裝置 200（圖 2）中所實施的方法步驟的實例。

從步驟 503 開始，密鑰管理邏輯 221 透過用戶獲得網路配置和聚合式網路密碼。例如，用戶可打開由網路裝置 200 的作業系統提供的圖形用戶介面配置對話。或者，網路裝置 200 可具有集成的螢幕和輸入裝置，以便用戶指定網路配置和聚合式網路密碼。

在步驟 506 中，密鑰管理邏輯 221 從聚合式網路密碼生成用於一個網路介面 212 的介面密碼。網路裝置 200 的不同網路介面 212 可具有不同的密碼尺寸要求。在一個實施方式中，密鑰管理邏輯 221 首先使用散列函數生成一個具有所要求的最大尺寸的密碼，其次對於各網路介面 212 根據需要縮短密碼。在另一個實施方式中，密鑰管理邏輯 221 使用散列函數從單個聚合式網路密碼中為每個不同的網路介面 212 生成單獨的密碼。所使用的散列函數可為單向散列，使得從介面密碼不可得到聚合式網路密碼。在各種實施方式中，相同網路類型的所有網段 412（圖 4）可採用相同的介面密碼，但在其他實施方式中，對於相同網路類型的不同網段 412 可採用不同的介面密碼。

在步驟 509 中，使用至少部分從聚合式網路密碼生成的介面密碼來配對網路介面 212。使用網路介面 212 的鏈路層技術的本地安全/保密協定來配對網路介面 212。透過本

地安全/保密協議可獲得額外的安全參數，並且該參數可由密鑰管理邏輯 221 儲存在網路密鑰 224 中。在步驟 512 中，密鑰管理邏輯 221 確定另一個網路介面 212 在網路裝置 200 中是否有效。如果另一個網路介面 212 有效，那麼密鑰管理邏輯 221 返回步驟 506，並且生成用於要配對的下一個網路介面 212 的介面密碼。否則，結束密鑰管理邏輯 221 的該部分。

請參照圖 6，圖 6 示出了根據各種實施方式的密鑰管理邏輯 221（圖 2）的一部分的操作的另一實例的流程圖。具體地，圖 6 涉及利用按鈕配對和密鑰分佈在聚合式網路 100（圖 1）中提供配對的實施方式。應理解的是，圖 6 的流程圖提供了可用於實施文中所述的密鑰管理邏輯 221 的一部分的多種不同類型的功能配置的僅僅一個實例。另外，圖 6 的流程圖可被視為描述根據一個或多個實施方式的網路裝置 200（圖 2）中所實施的方法步驟的實例。

從步驟 603 開始，密鑰管理邏輯 221 從網路裝置 200 的配對裝置 215（圖 1）中獲得配對事件，例如物理或邏輯按鈕的按下等。在步驟 606 中，密鑰管理邏輯 221 使用網路介面 212 所使用的鏈路層技術的本地配對協定為網路介面 212（圖 1）進行配對。通過該任務，可為網路介面 212 生成網路密鑰 224（圖 1）。在步驟 609 中，密鑰管理邏輯 221 確定是否已經發生超時。例如，雖然在網路裝置 200 中可生成配對事件，但是情況可能如下，在預定的時間長度到期之前，從聚合式網路 100 的遠端網路裝置 200 接收不到相應的配對事件。如果發生超時，則鏈路配對失效，密鑰管理邏輯 221 的該部分結束。

如果不發生超時，那麼密鑰管理邏輯 221 繼續至步驟 612。在步驟 612 中，密鑰管理邏輯 221 確定是否使用了集中式密鑰分佈。如果使用了集中式密鑰分佈，那麼密鑰管理邏輯 221 繼續至步驟 615，並且將配對產生的任何網路密鑰 224 提供給閘道 109（圖 1）。在步驟 618 中，密鑰管理邏輯 221 可從閘道 109 獲得網路密鑰 224，用於網路裝置 200 的其他有效網路介面 212。密鑰管理邏輯 221 繼續至框 621。

如果密鑰管理邏輯 221 在步驟 612 中確定未使用集中式密鑰分佈，那麼代替使用了密鑰分佈的分散式方式，並且密鑰管理邏輯 221 從步驟 612 轉換至步驟 624。在步驟 624 中，密鑰管理邏輯 221 向與其配對的其他網路裝置 200 公告該網路裝置 200 的網路密鑰 224。在步驟 627 中，密鑰管理邏輯 221 為網路裝置 200 的未配對鏈路請求網路密鑰 224。該請求可通過聚合式網路 100 從網路裝置 200 傳播開。最後，密鑰管理邏輯 221 通過已配對的中繼器 106（圖 1）獲得丟失的網路密鑰 224。密鑰管理邏輯 221 繼續至步驟 621。

在步驟 621 中，密鑰管理邏輯 221 確定是否存在可利用新的可用的網路密鑰 224 被配對的網路裝置 200 的其他網路介面 212。如果是的話，在步驟 633 中密鑰管理邏輯 221 發起網路介面 212 的配對。密鑰管理邏輯 221 繼續至步驟步驟 636。如果沒有其他的網路介面 212 進行配對，那麼密鑰管理邏輯 221 也繼續至步驟 636。在步驟 636 中，密鑰管理邏輯 221 確定網路裝置 200 的另一個網路介面 212 是否變得有效。例如，用戶可將 USB Wi-Fi 網路介面 212 或

者其他可插入式網路介面 212 插入網路裝置 200。如果另一個網路介面 212 已經變得有效，那麼密鑰管理邏輯 221 返回至步驟 612，並且繼續獲得用於網路介面 212 的網路密鑰 224。否則，密鑰管理邏輯 221 的該部分結束。

請參照圖 7，圖 7 示出了根據各種實施方式的密鑰分佈邏輯 118（圖 1）的一部分的操作的一個實例的流程圖。應理解的是，圖 7 的流程圖提供可用於實現文中所述的密鑰分佈邏輯 118 的一部分的操作的多種不同類型的功能配置的僅僅一個實例。另外，圖 7 的流程圖可被視為描述根據一個或多個實施方式的閘道 109（圖 1）中所實施的方法步驟的實例。

從步驟 703 開始，密鑰分佈邏輯 118 發現新的網路裝置 200（圖 2），該裝置已經添加到聚合式網路 100（圖 1）的網路拓撲 124（圖 1）中。在步驟 706 中，密鑰分佈邏輯 118 獲得透過配對新的網路裝置 200 而得到的網路密鑰 224（圖 2）。網路密鑰 224 可儲存在網路密鑰 121（圖 1）中，該網路密鑰 121 可將網路密鑰 224 映射到網路拓撲 124 中。

在步驟 709 中，密鑰分佈邏輯 118 確定新的網路裝置 200 是否具有其他未配對的網路介面 212（圖 2）。例如，密鑰分佈邏輯 118 可從網路裝置 200 獲得對用於其未配對的網路介面 212 的網路密鑰 224 的請求。如果是的話，密鑰分佈邏輯 118 將合適的網路密鑰 224 提供給新的網路裝置 200，如果可用的話，用於新的網路裝置 200 所支援的其他網路介面 212。密鑰分佈邏輯 118 繼續至步驟 715。如果新的網路裝置 200 沒有其他未配對的網路介面 212，則密鑰分

佈邏輯 118 也從步驟 709 繼續至步驟 715。

在步驟 715 中，作為配對新的網路裝置 200 的結果，密鑰分佈邏輯 118 確定新的網路密鑰 224 是否已經添加到網路密鑰 121 中。如果已經添加了新的網路密鑰 224，那麼密鑰分佈邏輯 118 為連接到聚合式網路 100 的其他網路裝置 200 提供新的網路密鑰 224，其他網路裝置 200 支援與新的網路密鑰 224 相關的各種網路介面 212。密鑰分佈邏輯 118 繼續至步驟 721。如果未添加新的網路密鑰 224，那麼密鑰分佈邏輯 118 從步驟 715 轉換到步驟 721。

在步驟 721 中，密鑰分佈邏輯 118 確定另一個新的網路裝置 200 是否已經添加到聚合式網路 100 中。如果已經添加了另一個新的網路裝置 200，那麼密鑰分佈邏輯 118 返回至步驟 703。如果沒有添加新的網路裝置 200，那麼密鑰分佈邏輯 118 的該部分結束。

請參照圖 8，圖 8 示出了根據各種實施方式的密鑰管理邏輯 221（圖 2）的一部分的操作的另一個實例的流程圖。具體地來說，圖 8 涉及基於配對事件的獲得來中繼配對事件以及發起配對。應理解的是，圖 8 的流程圖提供了可用於實施文中所述的密鑰管理邏輯 221 的一部分的操作的多種不同類型的功能配置的僅僅一個實例。另外，圖 8 的流程圖可被視為描述根據一個或多個實施方式的網路裝置 200（圖 2）中實施的方法步驟的實例。

從步驟 803 開始，密鑰管理邏輯 221 獲得配對事件。配對事件可為本地物理或邏輯按鈕的按下，或者可從聚合式網路 100（圖 1）上的另一個網路裝置 200 獲得。在步驟 806 中，密鑰管理邏輯 221 通過網路裝置 200 的其他網路介

面 212（圖 2）中繼配對事件。在步驟 809 中，密鑰管理邏輯 221 確定是否存在連接到網路裝置 200 的未配對的網路裝置 200。如果不存在連接到網路裝置 200 的未配對的網路裝置 200，那麼密鑰管理邏輯 221 的該部分結束。

另外，如果存在連接到網路裝置 200 的未配對的網路裝置 200，那麼取而代之密鑰管理邏輯 221 前進至步驟 812。在步驟 812 中，密鑰管理邏輯 221 確定在超時之前，是否從未配對的網路裝置 200 獲得相應的配對事件。可在步驟 803 中獲得的配對事件之前或之後獲得這種相應的配對事件，但是兩個配對事件之間的時間長度限於預定的時間長度。如果發生超時，那麼密鑰管理邏輯 221 的該部分結束，而不為未配對的網路裝置 200 配對。

如果未發生超時，那麼取而代之密鑰管理邏輯 221 轉換至步驟 815，並且使用其他網路裝置 200 的未配對的網路介面 212 的本地配對事件協定（例如按鈕配對協定或其他協定）與其他網路裝置 200 進行配對。要注意的是，未配對的網路裝置 200 可具有多個網路介面 212。在各種實施方式中，未建立任何配對優先順序。一旦一個網路介面 212 被配對，那麼對應於未配對的網路介面 212 的網路密鑰 224 可通過被配對的網路介面 212 分佈給其他網路裝置 200。之後，密鑰管理邏輯 221 的該部分結束。

參看圖 9A 至圖 9C，圖 9A 至圖 9C 示出了在聚合式網路 100（圖 1）中使用由閘道 109（圖 1）集中的網路密鑰分佈的網路裝置 200（圖 2）之間的網路密鑰分佈的一個實例的序列圖。採用圖 1 的實例中給出的聚合式網路 100 的樣本拓撲。在圖 9A 至圖 9C 中，矩形表示乙太網路介面 212

（圖 2），三角形表示 PLC 網路介面 212，菱形表示 Wi-Fi 網路介面 212，五角形表示 MoCA 網路介面 212。各個形狀內的“K”表示配對的介面，而各個形狀內沒有“K”表示未配對的介面。

從圖 9A 開始，最初通過乙太網路介面 212 在聚合式網路 100 中配對閘道 109 和中繼器 106a。中繼器 106a 也具有未配對的 PLC 和 MoCA 網路介面 212。在時間 900 處，中繼器 106b 加入聚合式網路 100。中繼器 106b 最初具有未配對的 PLC 和 Wi-Fi 網路介面 212。在時間 903 處，中繼器 106b 經由 PLC 網路介面 212 的本地配對協定與中繼器 106a 配對。生成和交換網路密鑰 224（圖 2）。在時間 906 處，用於 PLC 網段 412（圖 4）的網路密鑰 224 被發送回閘道 109。這樣，在時間 906 後，網路密鑰 121 包括用於乙太網路和 PLC 網路介面的安全/保密參數。

接下來，在圖 9B 中，在時間 912 處，中繼器 106c 加入聚合式網路 100。最初，中繼器 106c 具有未配對的 MoCA 和 Wi-Fi 網路介面 212。在時間 915 處，中繼器 106c 通過 Wi-Fi 網路介面 212 的本地配對協定與中繼器 106b 配對。生成和交換網路密鑰 224。在時間 918 處，通過中繼器 106a 將用於 Wi-Fi 網段 412 的網路密鑰 224 發送回閘道 109。這樣，在時間 918 後，網路密鑰 121 包括用於乙太網路、PLC 以及 Wi-Fi 網路介面 212 的安全/保密參數。

在圖 9C 中，在時間 921 處，終端 103c 加入聚合式網路 100。最初，終端 103c 具有未配對的 MoCA 和 PLC 網路介面 212。在時間 924 處，終端 103c 經由 MoCA 網路介面 212 的本地配對協定與中繼器 106c 配對。生成和交換網路

密鑰 224。在時間 927 處，通過中繼器 106a 和中繼器 106b 將用於 MoCA 網段 412 的網路密鑰 224 發送回閘道 109。這樣，在時間 927 後，網路密鑰 121 包括用於乙太網路、PLC、Wi-Fi 以及 MoCA 網路介面的安全/保密參數。

在時間 930 處，閘道 109 為中繼器 106a 提供 MoCA 安全/保密參數。在時間 933 處，中繼器 106a 的 MoCA 網路介面 212 使用閘道 109 所提供的安全/保密參數，與中繼器 106c 的 MoCA 網路介面 212 配對。在時間 936 處，閘道 109 為終端 103c 提供 PLC 安全/保密參數。在時間 939 處，終端 103c 的 PLC 網路介面 212 使用閘道 109 所提供的安全/保密參數，與中繼器 106a 的 PLC 網路介面 212 配對。要注意的是，可在時間 930 處傳送 MoCA 參數之前，在時間 936 處傳送 PLC 參數，以及可在時間 933 處進行配對之前，在時間 939 處進行配對。而且，雖然在圖 9A 至圖 9C 中按順序示出了某些任務，但是應理解，在其他實施方式中，它們可並行地或者以其他的順序發生。

參看圖 10，圖 10 示出了在聚合式網路 100（圖 1）中使用分散的網路密鑰分佈的網路裝置 200（圖 2）之間的網路密鑰分佈的一個實例的序列圖。使用圖 1 的實例中給出的聚合式網路 100 的樣本拓撲。在圖 10 中，矩形表示乙太網路介面 212（圖 2），三角形表示 PLC 網路介面 212，菱形表示 Wi-Fi 網路介面 212，五角形表示 MoCA 網路介面 212。各個形狀內的“K”表示配對的介面，各個形狀內沒有“K”表示未配對的介面。

最初，在時間 1000 處，在聚合式網路 100 中配對了中繼器 106a、106b 和 106c。中繼器 106a 具有配對的乙太網

路和 PLC 網路介面 212 以及未配對的 MoCA 網路介面 212。中繼器 106b 具有配對的 PLC 和 Wi-Fi 網路介面 212。中繼器 106c 具有配對的 Wi-Fi 網路介面 212 和未配對的 MoCA 網路介面 212。終端 103c 具有未配對的 PLC 和 MoCA 網路介面 212。

在時間 1003 處，通過將其 MoCA 網路介面 212 與中繼器 106c 的 MoCA 網路介面 212 配對，終端 103c 加入聚合式網路 100。生成和交換網路密鑰 224。在時間 1006 處，通過聚合式網路 100，用於 MoCA 網段 412（圖 4）的安全/保密參數被傳送給中繼器 106b 和中繼器 106a。也傳送對 PLC 安全/保密參數的請求。在時間 1009 處，使用在時間 1006 處傳送的用於 MoCA 網段 412 的安全/保密參數，中繼器 106a 的 MoCA 網路介面 212 被配對。

在時間 1012 處，中繼器 106b 回應於對 PLC 安全/保密參數的請求，並且通過中繼器 106c 將 PLC 參數發送給終端 103c。在時間 1015 處，終端 103c 的 PLC 網路介面 212 使用在時間 1012 處獲得的 PLC 參數進行了配對。雖然在圖 10 中按照順序示出了某些任務，但是可理解的是，在其他實施方式中，它們可並行地或者以其他的順序發生。

繼續看圖 11，圖 11 示出了說明在聚合式網路 100（圖 1）中關於配對事件在網路裝置 200（圖 2）之間進行配對的序列圖。採用圖 1 的實例中給出的聚合式網路 100 的樣本拓撲。在圖 11 中，矩形表示乙太網路介面 212（圖 1），五角形表示 MoCA 網路介面 212。各個形狀內的“K”表示配對的介面，各個形狀內沒有“K”表示未配對的介面。

最初，在時間 1100 處，通過乙太網路和 MoCA 網路介

面 212，在聚合式網路 100 中，將閘道 109 和中繼器 106a 和 106b 進行配對。在時間 1100 處，在未配對的終端 103c 中產生配對事件（例如物理或邏輯按鈕的按下等）。在時間 1103 處，在閘道 109 中生成配對事件並且通過乙太網路鏈路將該配對事件發送給中繼器 106a。在時間 1106 處，中繼器 106a 複製配對事件並且通過 MoCA 鏈路將其轉發給中繼器 106b。在時間 1109 處，中繼器 106b 從中繼器 106a 獲得配對事件。

假設時間 1100 和時間 1109 之間的時間不滿足超時閾值，則在時間 1112 處中繼器 106b 使用 MoCA 介面的本地配對協定與終端 103c 進行配對。可生成用於 MoCA 網段 412（圖 1）的安全/保密參數。在時間 1115 處，終端 103c 的 MoCA 網路介面被配對至聚合式網路 100。

返回看圖 2 和圖 3，應理解的是，可存在其他應用程式，這些應用程式儲存在記憶體 206、306 中，並且可由處理器 203、303 執行，如可意識到的那樣。當以軟體的形式執行文中所討論的任何元件時，可使用多種程式語言中的任何一種語言，例如 C、C++、C#、Objective C、Java®、JavaScript®、Perl、PHP、Visual Basic®、Python®、Ruby、Delphi®、Flash®，或者其他程式語言。

多個軟體元件儲存在記憶體 206、306 中，並且可由處理器 203、303 執行。在這方面，術語“可執行”表示程式檔，該程式檔具有最終可由處理器 203、303 運行的形式。可執行的程式的實例例如可為編譯程序，該編譯程序可轉換成機器代碼，該機器代碼具有可被載入進記憶體 206、306 的隨機存取部分中的形式並且可由處理器 203、303 運行；

該編譯程序還可轉換成可用適當的格式表達的源代碼，例如能夠被載入進記憶體206、306的隨機存取部分中並且由處理器203、303執行的目標代碼；或者該編譯程序可轉換成可由另一可執行程式解釋的源代碼，以在記憶體206、306的隨機存取部分中生成指令，從而由處理器203、303執行；等等。可執行程式可儲存在記憶體206、306的任何部分或元件中，記憶體206、306例如包括隨機存取記憶體(RAM)、唯讀記憶體（ROM)、硬碟驅動器、固態驅動器、USB快閃記憶體盤、存儲卡、光碟（例如壓縮盤（CD）或數位化通用磁片（DVD))、軟碟、磁帶或其他記憶體元件。

記憶體206、306文中限定為包括易失性和非易失性記憶體和數位儲存元件。易失性組件為那些掉電時不保留資料值的元件。非易失性組件為那些掉電時保留資料值的元件。因此，記憶體206、306例如可包括隨機存取記憶體（RAM)、唯讀記憶體（ROM)、硬碟驅動器、固態驅動器、USB 快閃記憶體盤、通過讀卡器訪問的存儲卡、通過相關聯的軟碟驅動器訪問的軟碟、通過光碟驅動器訪問的光碟、通過合適的磁帶驅動器訪問的磁帶和/或其他記憶體元件、或這些記憶體元件中的兩個以上元件的組合。此外，RAM例如可包括靜態隨機存取記憶體（SRAM)、動態隨機存取記憶體（DRAM）或磁性隨機存取記憶體（MRAM）以及其他這種裝置。ROM例如可包括可編程唯讀記憶體(PROM)、可擦可編程唯讀記憶體（EPROM)、電可擦可編程唯讀記憶體（EEPROM）或者其他類似的記憶體裝置。

同樣，處理器 203、303 可表示多個處理器 203、303，並且記憶體206、306可表示分別在並行處理電路中操作

的多個記憶體 206、306。在這種情況下，本地介面 209、309 可為合適的網路，該網路有助於在多個處理器 203、303 的任何兩個之間、任何處理器 203、303 和任何記憶體 206、306 之間、或者任何兩個記憶體 206、306 之間等進行通信。本地介面 209、309 可包括被設計成協調該通信的其他系統，例如包括執行負載平衡。處理器 203、303 可為電力或一些其他可用的結構。

雖然閘道系統 115、MAC 抽象層 218、密鑰管理邏輯 221、密鑰分佈邏輯 118 以及文中所述的各種其他系統可被實現為上述通用硬體執行的軟體或代碼，但是作為選擇，也可被實現為專用硬體或軟體/通用硬體和專用硬體的組合。如果實現為專用硬體，則每個均可被實施為採用多種技術中的任何一種技術或多種技術的組合的電路或狀態機。這些技術可包括但不限於，具有用於在被施加一個或多個資料信號時實施各種邏輯功能的邏輯門的離散邏輯電路、具有適當的邏輯門的專用積體電路，或其他組件等。本領域技術人員通常熟知這樣的技術，因此文中不詳述。

圖 5 至圖 8 的流程圖示出了密鑰管理邏輯 221 和密鑰分佈邏輯 118 的一部分的實施形式的功能和操作。如果實現為軟體，則每個塊可表示代碼的一個模組、區段或部分，該代碼包括程式指令，以實施特定的邏輯功能。程式指令可被實現為源代碼或機器代碼的形式，源代碼包括以編程語言或機器代碼編寫的人類可讀的語句，機器代碼包括適當的執行系統（例如電腦系統中的處理器 203、303 或其他系統）可識別的數位指令。可從源代碼等轉換機器代碼。如果實現為硬體，那麼每個塊可表示一個電路或多個互

連的電路，以便執行特定的邏輯功能。

雖然圖 5 至圖 8 的流程圖示出了特定的執行順序，但是應理解，該執行順序可與所描繪的順序不同。例如，相對於所示出的順序，兩個或更多個塊的執行順序可被打亂。並且，可同時或部分同時執行圖 5 至圖 8 中連續示出的兩個或更多個塊。此外，在一些實施方式中，可跳過或省略圖 5 至圖 8 中示出的一個或多個塊。此外，為了增強效用、進行結算、性能測量或幫助排除故障等，可將任何數量的計數器、狀態變數、警告信號機或消息添加到文中所述的邏輯流中。應理解，所有這種變化均在本發明的範圍內。

並且，文中所述的包括軟體或代碼的任何邏輯或應用程式可被實現為任何非瞬態電腦可讀介質，由指令執行系統使用或結合指令執行系統（例如電腦系統中的處理器 203、303 或其他系統）使用，該邏輯或應用程式包括閘道系統 115、MAC 抽象層 218、密鑰管理邏輯 221 以及密鑰分佈邏輯 118。從這個意義上來說，邏輯例如可包括包含指令和聲明的語句，這些語句可從電腦可讀介質中取得並且可由指令執行系統執行。在本發明的背景下，“電腦可讀介質”可為任何可包含、儲存或維持文中所述的邏輯或應用程式的介質，由指令執行系統使用或結合指令執行系統使用。電腦可讀介質可包括多種物理介質（例如磁性、光學或半導體介質）中的任何一種。適當的電腦可讀介質更具體的實例包括但不限於，磁帶、磁性軟碟、磁性硬碟驅動器、存儲卡、固態驅動器、USB 快閃記憶體盤或光碟。並且，電腦可讀介質可為隨機存取記憶體（RAM），例如包括靜態

隨機存取記憶體（SRAM）和動態隨機存取記憶體（DRAM），或磁性隨機存取記憶體（MRAM）。此外，電腦可讀介質可為唯讀記憶體（ROM）、可編程唯讀記憶體（PROM）、可擦可編程唯讀記憶體（EPROM）、電可擦可編程唯讀記憶體（EEPROM）或者其他類型的記憶體裝置。

要強調的是，本發明的上述實施方式僅是為了清楚地理解本發明的原理而提出的實現方式的可能實例。上述實施方式可進行多種變化和修改，而本質上不背離本發明的精神和原理。文中所有這些修改和變化均意在包含在本發明的範圍內，並且由所附權利要求保護。

【圖式簡單說明】

圖 1 為根據本發明的各種實施方式的聚合式網路的功能方塊圖。

圖 2 為提供根據本發明的各種實施方式的圖 1 的聚合式網路中所採用的網路裝置的一個實例圖示的示意性框圖。

圖 3 為提供根據本發明的各種實施方式的圖 1 的聚合式網路中所採用的閘道的一個實例圖示的示意性框圖。

圖 4 為根據本發明的各種實施方式的表示圖 1 的聚合式網路中所採用的分層網路模型的示意圖。

圖 5 至圖 8 為示出被實現為根據本發明的各種實施方式的作為圖 1 的聚合式網路中的網路裝置中執行的密鑰管理邏輯和/或密鑰分佈邏輯的部分的功能性實例的流程圖。

圖 9A 至圖 9C 為示出根據本發明的各種實施方式的圖 1 的聚合式網路中使用由閘道集中的網路密鑰分佈的網路

裝置之間的網路密鑰分佈的序列圖。

圖 10 為示出根據本發明的各種實施方式的圖 1 的聚合式網路中使用分散的網路密鑰分佈的網路裝置之間的網路密鑰分佈的序列圖。

圖 11 為示出根據本發明的各種實施方式圖 1 的聚合式網路中關於配對事件在網路裝置之間進行配對的序列圖。

【主要元件符號說明】

100：聚合式網路

103a、103b、103c：終端

106a、106b、106c：中繼器

112：網路

109：閘道

115：閘道系統

118：密鑰分佈邏輯

121：網路密鑰

124：網路拓撲

200：網路裝置

203、303：處理器

206、306：記憶體

209、309：本地介面

218：MAC 抽象層

221：密鑰管理邏輯

224：網路密鑰

212a~212N：網路介面

215：配對裝置

312：WAN 介面

400：分層網路模式

403：上層實體

406a~406N：MAC 類型

409a~409N：PHY 類型

412a~412N：網段

503~512、603~636、703~721、803~815：步驟流程

900~906、912~918、921~939、1000~1015、1100~1115：時間點

七、申請專利範圍：

1. 一種用於生成和分佈網路安全參數的系統，包括：

多個網路裝置，透過採用多種異構鏈路層技術的一聚合式資料通信網路進行資料通信；並且

其中，所述網路裝置中的至少一個網路裝置包括到所述聚合式資料通信網路的多個網路介面，所述網路介面中的一第一網路介面採用所述異構鏈路層技術中的一第一異構鏈路層技術，所述網路介面中的一第二網路介面採用所述異構鏈路層技術中的一第二異構鏈路層技術，並且所述網路裝置中的所述至少一個網路裝置進一步包括一網路安全參數管理邏輯，所述網路安全參數管理邏輯被配置為：

獲得聚合式網路密碼；以及

透過至少部分地基於所述聚合式網路密碼、使用相應的一種異構鏈路層技術的本地配對協定為所述網路介面中的一個網路介面配對，以連接至所述聚合式資料通信網路；

其中所述網路裝置中的所述至少一個網路裝置進一步包括一網路安全參數分佈邏輯，所述網路安全參數分佈邏輯被配置為：

獲得對於所述網路安全參數的一請求，所述請求來自所述網路裝置中的另一網路裝置；

確定所述網路安全參數是否與所述網路介面

中的至少一個網路介面相關；

當所述網路安全參數與所述網路介面中的所述至少一個網路介面相關時，透過所述聚合式資料通信網路將所述網路安全參數發送至所述網路裝置中的所述另一網路裝置；以及

當所述網路安全參數與所述網路介面中的所述至少一個網路介面不相關時，將所述請求在所述聚合式資料通信網路中從所述網路裝置中的所述另一網路裝置傳播開。

2. 如申請專利範圍第 1 項所述之系統，其中所述網路安全參數管理邏輯進一步被配置為：

至少部分地基於所述聚合式網路密碼，生成用於所述網路介面中的所述第一網路介面的一第一網路密碼；以及

至少部分地基於所述聚合式網路密碼，生成用於所述網路介面中的所述第二網路介面的一第二網路密碼。

3. 如申請專利範圍第 2 項所述之系統，其中透過將各自的散列函數應用於所述聚合式網路密碼，以單獨地生成所述第一網路密碼和所述第二網路密碼。

4. 如申請專利範圍第 2 項所述之系統，其中透過將散列函數應用於所述聚合式網路密碼來生成所述第一網路密碼，並且透過縮短所述第一網路密碼來生成所述第二網路密碼。

5. 如申請專利範圍第 1 項所述之系統，其中所述網路介面中的所述一個網路介面是所述網路介面中的所述第一網路介面，所述網路安全參數管理邏輯進一步被配置為：透過至少部分地基於所述聚合式網路密碼、使用所述異構鏈路層技術中的所述第二異構鏈路層技術的另一本地配對協定為所述網路介面中的所述第二網路介面配對，以連接至所述聚合式資料通信網路。

6. 如申請專利範圍第 1 項所述之系統，其中所述網路介面中的所述一個網路介面是所述網路介面中的所述第一網路介面，並且所述網路安全參數管理邏輯進一步被配置為：

透過所述網路介面中的所述第一網路介面，獲得一網路安全參數，用於為所述網路介面中的所述第二網路介面配對；以及

透過至少部分地基於所述網路安全參數為所述網路介面中的所述第二網路介面配對，以連接至所述聚合式資料通信網路。

7. 如申請專利範圍第 1 項所述之系統，其中所述網路裝置中的所述至少一個網路裝置進一步包括一抽象層，所述抽象層被配置為：

從網路層獲得一第一資料訊框和一第二資料訊框；

透過所述網路介面中的所述第一網路介面將所述第一資料訊框路由至一目的地；以及

透過所述網路介面中的所述第二網路介面將所述第二資料訊框路由至所述目的地。

8. 如申請專利範圍第 7 項所述之系統，其中一媒體存取控

制位址被分配給所述抽象層，並且所述媒體存取控制位址在所述聚合式資料通信網路內是唯一的。

9. 一種用於生成和分佈網路安全參數的系統，包括：

多個網路裝置，透過採用多種異構鏈路層技術的一聚合式資料通信網路進行資料通信；以及

一閘道裝置，對應於所述網路裝置中的一第一網路裝置，所述閘道裝置包括一網路安全參數分佈邏輯，所述網路安全參數分佈邏輯被配置為：

獲得用於所述聚合式資料通信網路的多個網路部分中的每一個、採用所述異構鏈路層技術中的一第一異構鏈路層技術的所述網路部分中的第一網路部分、採用所述異構鏈路層技術中的一第二異構鏈路層技術的所述網路部分中的第二網路部分的所述網路安全參數，每個所述網路安全參數有助於到所述網路部分中的相應一個網路部分的受認證連接；

獲得來自所述網路裝置中的一第二網路裝置的對於所述網路安全參數中的至少一個網路安全參數的一請求；以及

通過所述聚合式資料通信網路將所述網路安全參數中的所述至少一個網路安全參數提供給所述網路裝置中的所述第二網路裝置。

10. 如申請專利範圍第 9 項所述之系統，其中所述閘道裝置

進一步包括維持連接至所述聚合式資料通信網路的所述網路裝置的拓撲的邏輯。

11. 如申請專利範圍第 9 項所述之系統，其中所述閘道裝置被配置為：將資料從所述聚合式資料通信網路路由至另一網路。

12. 如申請專利範圍第 9 項所述之系統，其中所述請求從所述網路裝置中的一第三網路裝置獲得，並且透過所述網路裝置中的所述第三網路裝置將所述網路安全參數中的所述至少一個網路安全參數提供給所述網路裝置中的所述第二網路裝置。

13. 如申請專利範圍第 9 項所述之系統，其中所述網路裝置中的至少一個網路裝置對應於具有多個第一網路介面的一中繼網路裝置，所述網路裝置中的至少一個網路裝置對應於具有多個第二網路介面的一終端網路裝置，所述中繼網路裝置被配置為在所述第一網路介面之間中繼管理訊框和資料訊框，所述終端網路裝置被配置為在所述第二網路介面之間中繼管理訊框而不中繼資料訊框。

14. 一種用於生成和分佈網路安全參數的方法，包括：

在多個網路裝置中的一第一網路裝置中生成一配對事件；

透過多種異構鏈路層技術中的一第一異構鏈路層技術，在所述網路裝置中的所述第一網路裝置中將所述配對事件分佈至所述聚合式資料通信網路；

透過所述聚合式資料通信網路，在所述多個網路裝置中的第二網路裝置中獲得所述配對事件；

使用所述異構鏈路層技術中的一第二異構鏈路層技

術的本地配對事件協議，透過所述異構鏈路層技術中的所述第二異構鏈路層技術，在所述網路裝置中的所述第二網路裝置中發起與所述網路裝置中的一第三網路裝置的配對；以及

其中，所述配對被配置為透過所述異構鏈路層技術中的所述第二異構鏈路層技術將所述網路裝置中的所述第三網路裝置連接至所述聚合式資料通信網路。

15. 如申請專利範圍第 14 項所述之方法，其中所述配對事件對應於於一按鈕事件，回應於用戶按下所述網路裝置中的所述第一網路裝置的按鈕，在所述網路裝置中的所述第一網路裝置中生成所述按鈕事件。

16. 如申請專利範圍第 14 項所述之方法，進一步包括在所述網路裝置中的所述第三網路裝置中請求所述聚合式資料通信網路上的所述網路安全參數，用於將所述網路裝置中的所述第三網路裝置與所述網路裝置中的第四網路裝置配對。

17. 如申請專利範圍第 14 項所述之方法，進一步：

在所述網路裝置中的所述第三網路裝置中生成另一配對事件；

在所述網路裝置中的所述第三網路裝置中，透過所述異構鏈路層技術中的所述第二異構鏈路層技術，將所述另一配對事件發送至所述網路裝置中的所述第二網路裝置；以及

其中，所述網路裝置中的所述第二網路裝置被配置為執行以下步驟：回應於在預定長度的時間內獲得

所述配對事件和所述另一配對事件，發起配對。

18.如申請專利範圍第 14 項所述之方法，進一步包括：

在多個網路裝置中的一第四網路裝置中，透過所述聚合式資料通信網路獲得所述配對事件；

使用所述異構鏈路層技術中的一第三異構鏈路層技術的本地配對事件協議，透過所述異構鏈路層技術中的所述第三異構鏈路層技術，在所述網路裝置中的所述第四網路裝置中發起與所述網路裝置中的所述第三網路裝置的另一配對；以及

其中，所述另一配對被配置為透過所述異構鏈路層技術中的所述第三異構鏈路層技術將所述網路裝置中的所述第三網路裝置連接至所述聚合式資料通信網路。

19.如申請專利範圍第 14 項所述之方法，進一步包括：

使用所述異構鏈路層技術中的所述第三異構鏈路層技術的本地配對事件協議，透過所述異構鏈路層技術中的所述第三異構鏈路層技術，在所述網路裝置中的所述第二網路裝置中發起與所述網路裝置中的所述第三網路裝置的另一配對；以及

其中，所述另一配對被配置為通過所述異構鏈路層技術中的所述第三異構鏈路層技術將所述網路裝置中的所述第三網路裝置連接至所述聚合式資料通信網路。

八、 圖式：

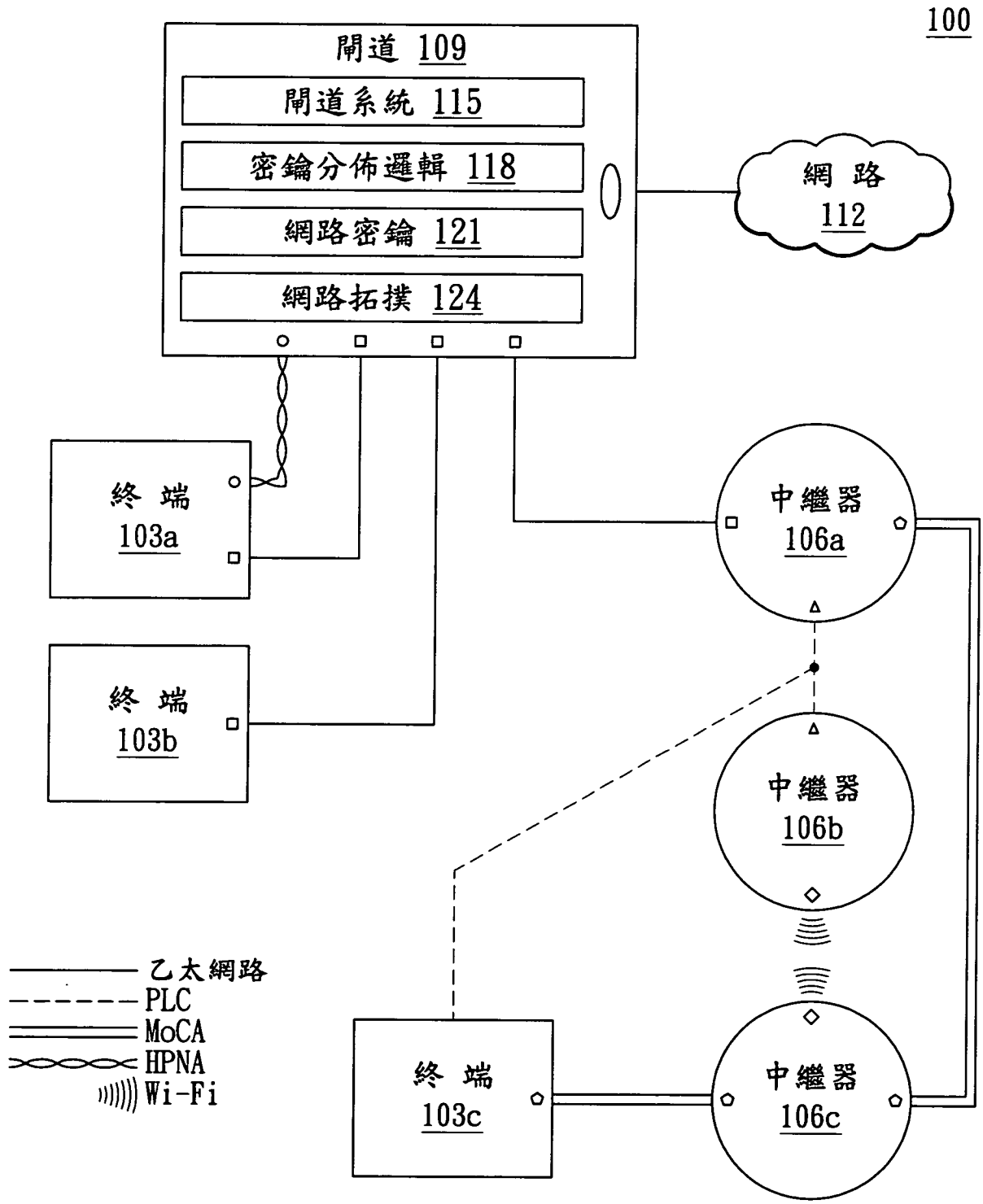
100
閘道 109
閘道系統 115
密鑰分佈邏輯 118
網路密鑰 121
網路拓撲 124
網 路
112
終 端
103a
終 端
103b
終 端
103c
中繼器
106a
中繼器
106b
中繼器
106c
乙太網路
PLC
MoCA
HPNA
Wi-Fi

圖1

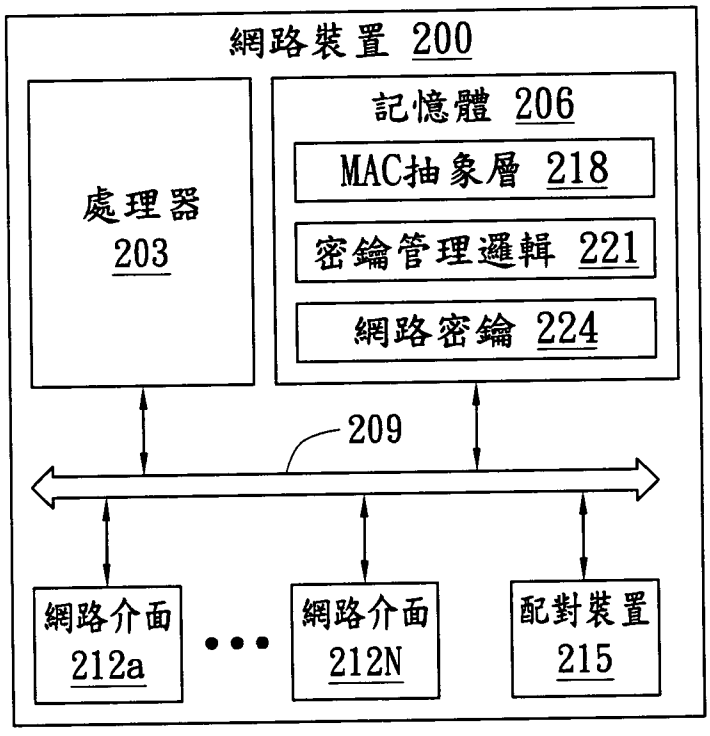
網路裝置 200
處理器
203
記憶體 206
MAC抽象層 218
密鑰管理邏輯 221
網路密鑰 224
209
網路介面
212a
網路介面
212N
配對裝置
215

圖2

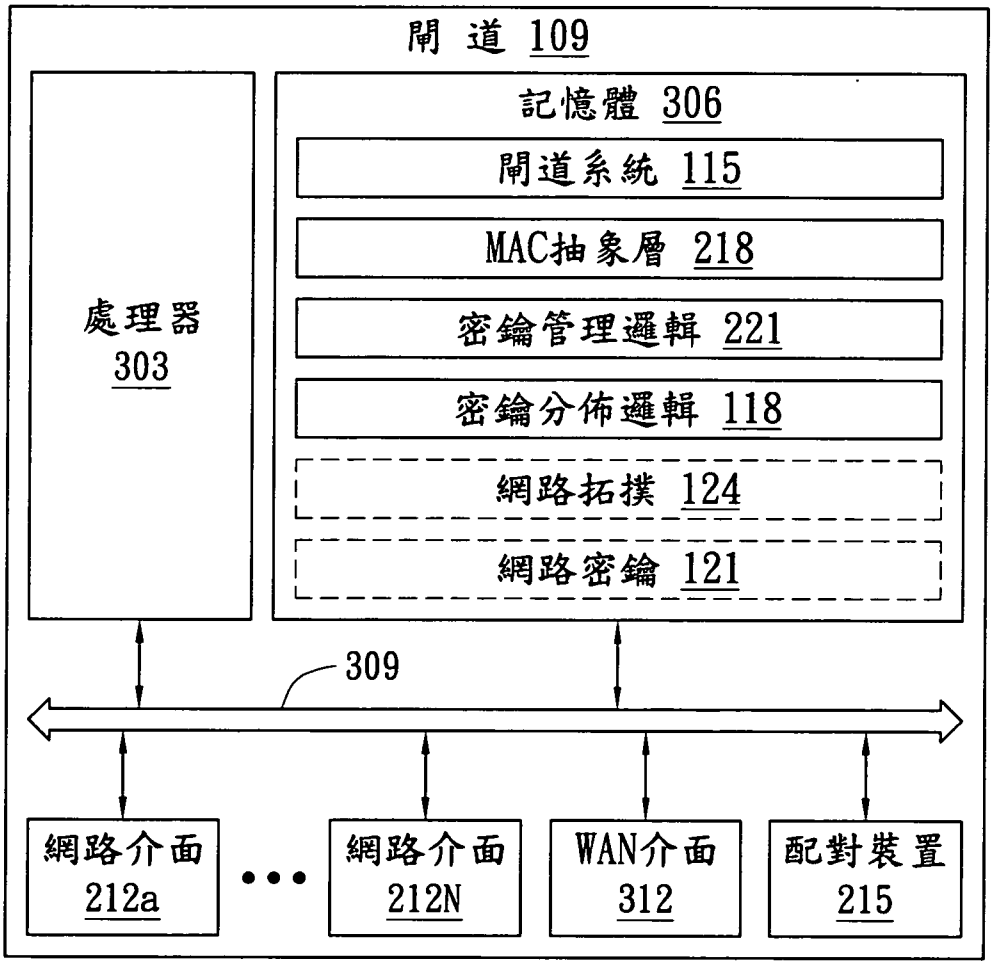
閘 道 109
處理器
303
記憶體 306
閘道系統 115
MAC抽象層 218
密鑰管理邏輯 221
密鑰分佈邏輯 118
網路拓撲 124
網路密鑰 121
309
網路介面
212a
網路介面
212N
WAN介面
312
配對裝置
215

圖3

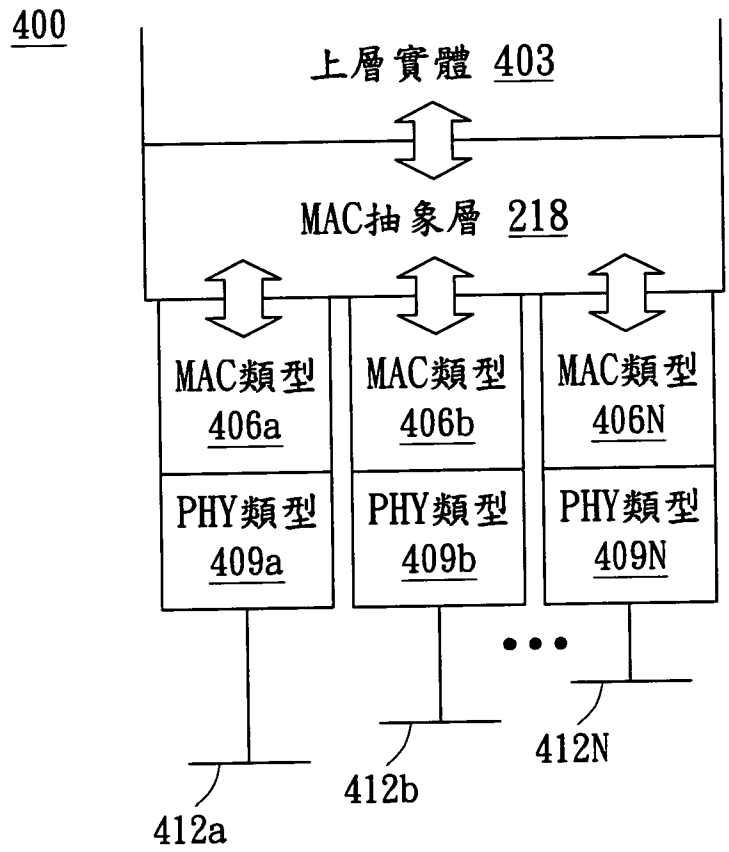
400
上層實體 403
MAC抽象層 218
MAC類型 406a
MAC類型 406b
MAC類型 406N
PHY類型 409a
PHY類型 409b
PHY類型 409N
412a
412b
412N

圖4

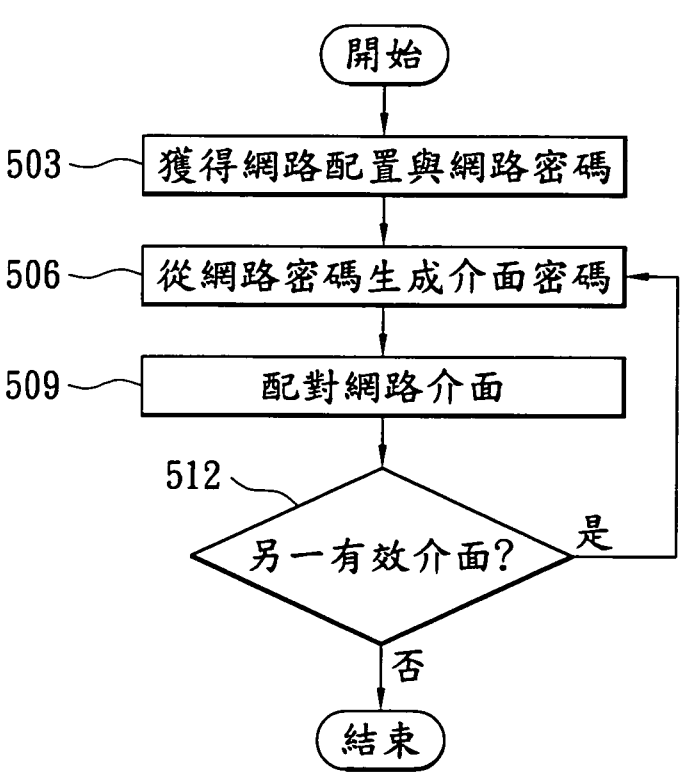
221
開始
503
獲得網路配置與網路密碼
506
從網路密碼生成介面密碼
509
配對網路介面
512
另一有效介面?
是
否
結束

圖5

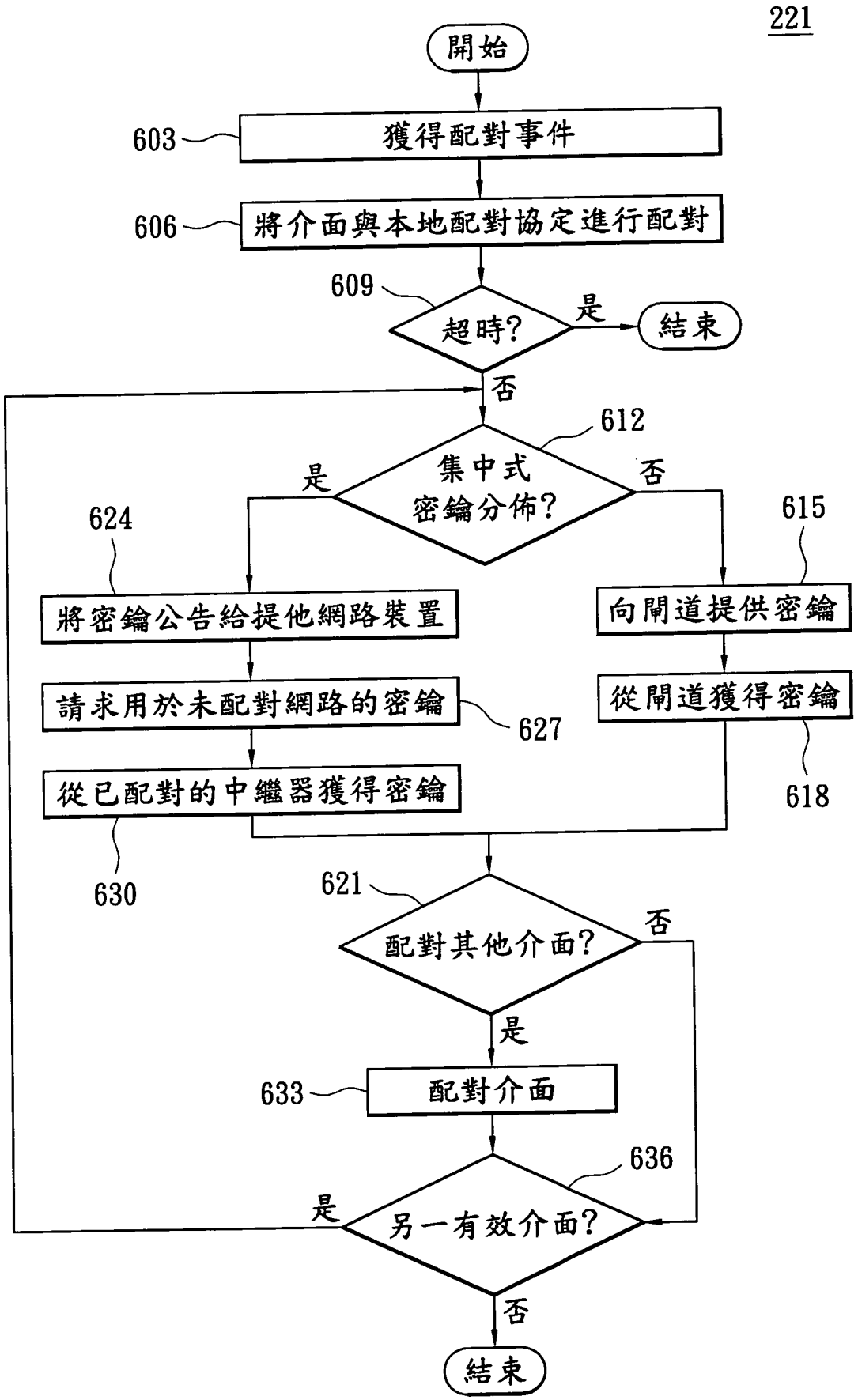
221
開始
603
獲得配對事件
606
將介面與本地配對協定進行配對
609
超時?
是
結束
否
612
集中式
密鑰分佈?
是
否
624
615
將密鑰公告給提他網路裝置
向閘道提供密鑰
請求用於未配對網路的密鑰
627
從閘道獲得密鑰
618
從已配對的中繼器獲得密鑰
630
621
配對其他介面?
否
是
633
配對介面
636
另一有效介面?
是
否
結束

圖6

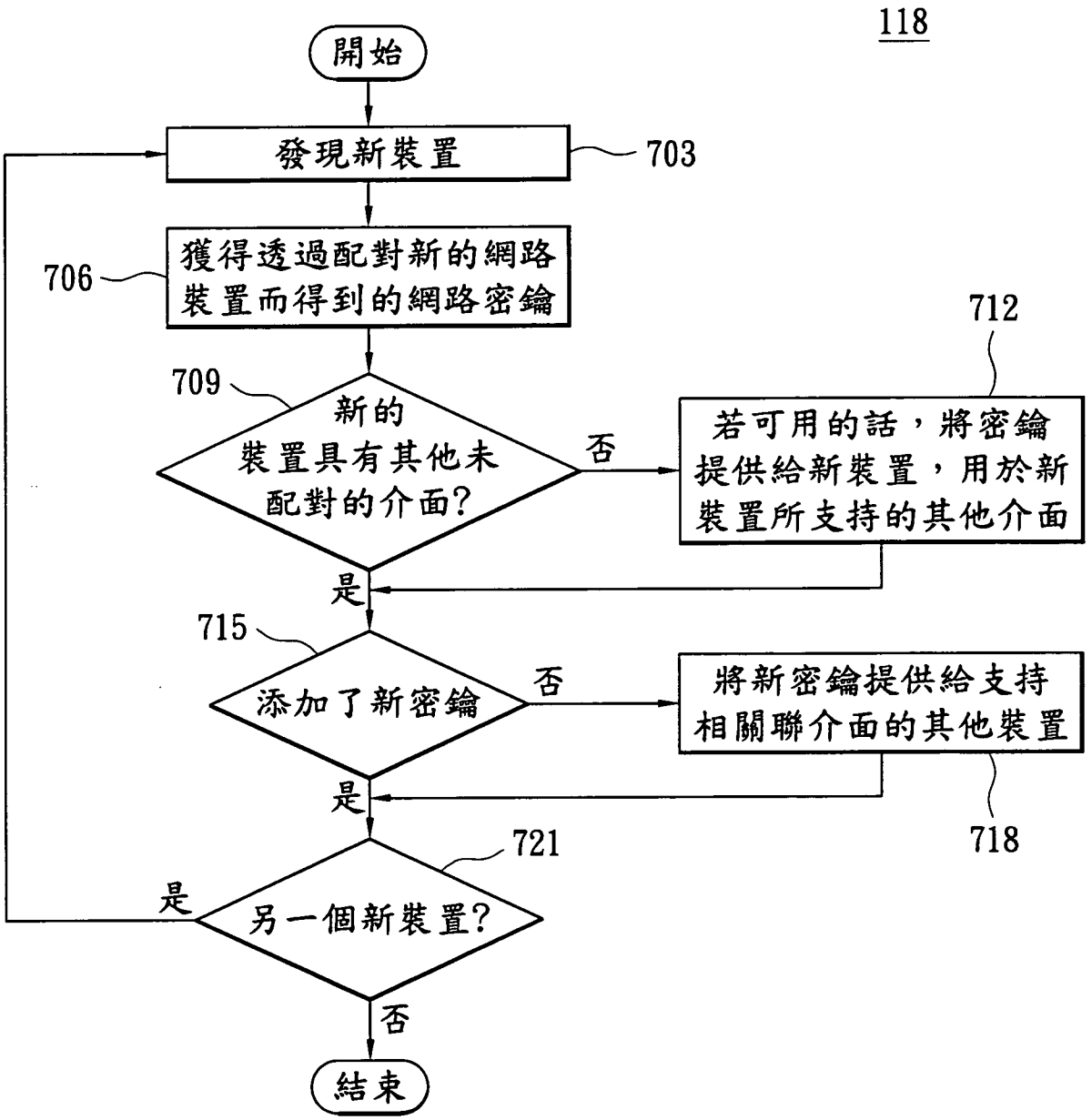
118
開始
發現新裝置
703
獲得透過配對新的網路裝置而得到的網路密鑰
706
709
新的裝置具有其他未配對的介面?
否
712
若可用的話，將密鑰提供給新裝置，用於新裝置所支持的其他介面
是
715
添加了新密鑰
否
將新密鑰提供給支持相關聯介面的其他裝置
718
是
721
是
另一個新裝置?
否
結束

圖7

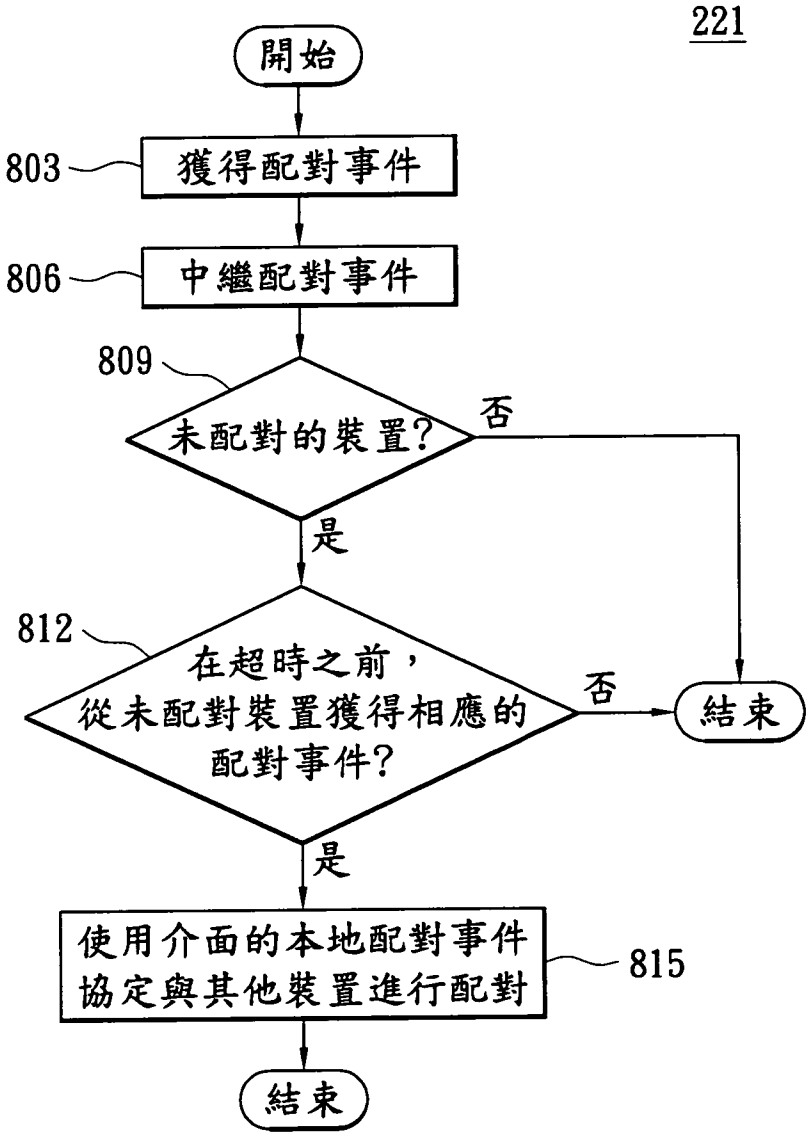
221
開始
803
獲得配對事件
806
中繼配對事件
809
未配對的裝置?
否
是
812
在超時之前，
從未配對裝置獲得相應的
配對事件?
否
結束
是
使用介面的本地配對事件
協定與其他裝置進行配對
815
結束

圖8

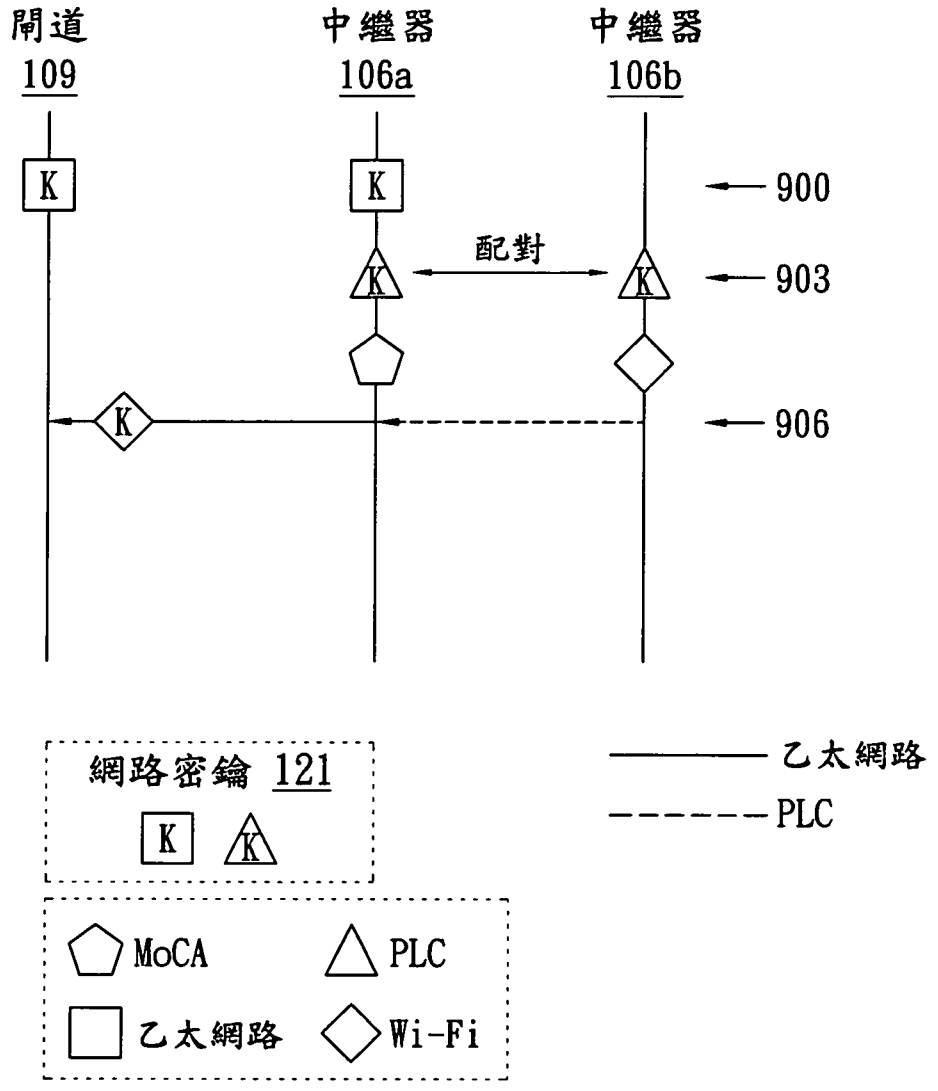
閘道
109
中繼器
106a
中繼器
106b
K
900
配對
903
906
網路密鑰 121
乙太網路
PLC
MoCA
PLC
乙太網路
Wi-Fi

圖9A

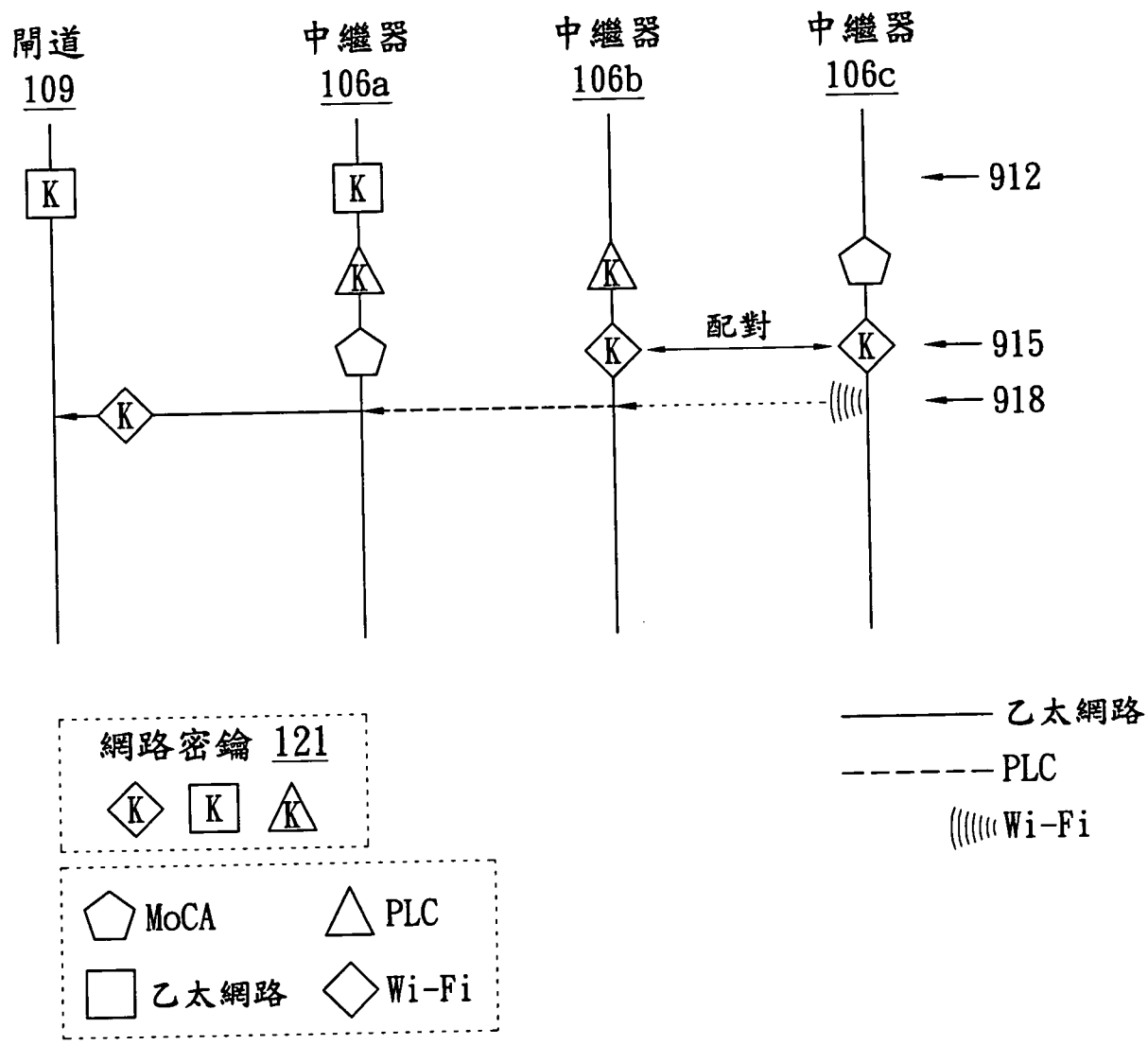
閘道
109
中繼器
106a
中繼器
106b
中繼器
106c
912
915
918
配對
K
網路密鑰 121
MoCA
PLC
乙太網路
Wi-Fi
乙太網路
PLC
Wi-Fi

圖9B

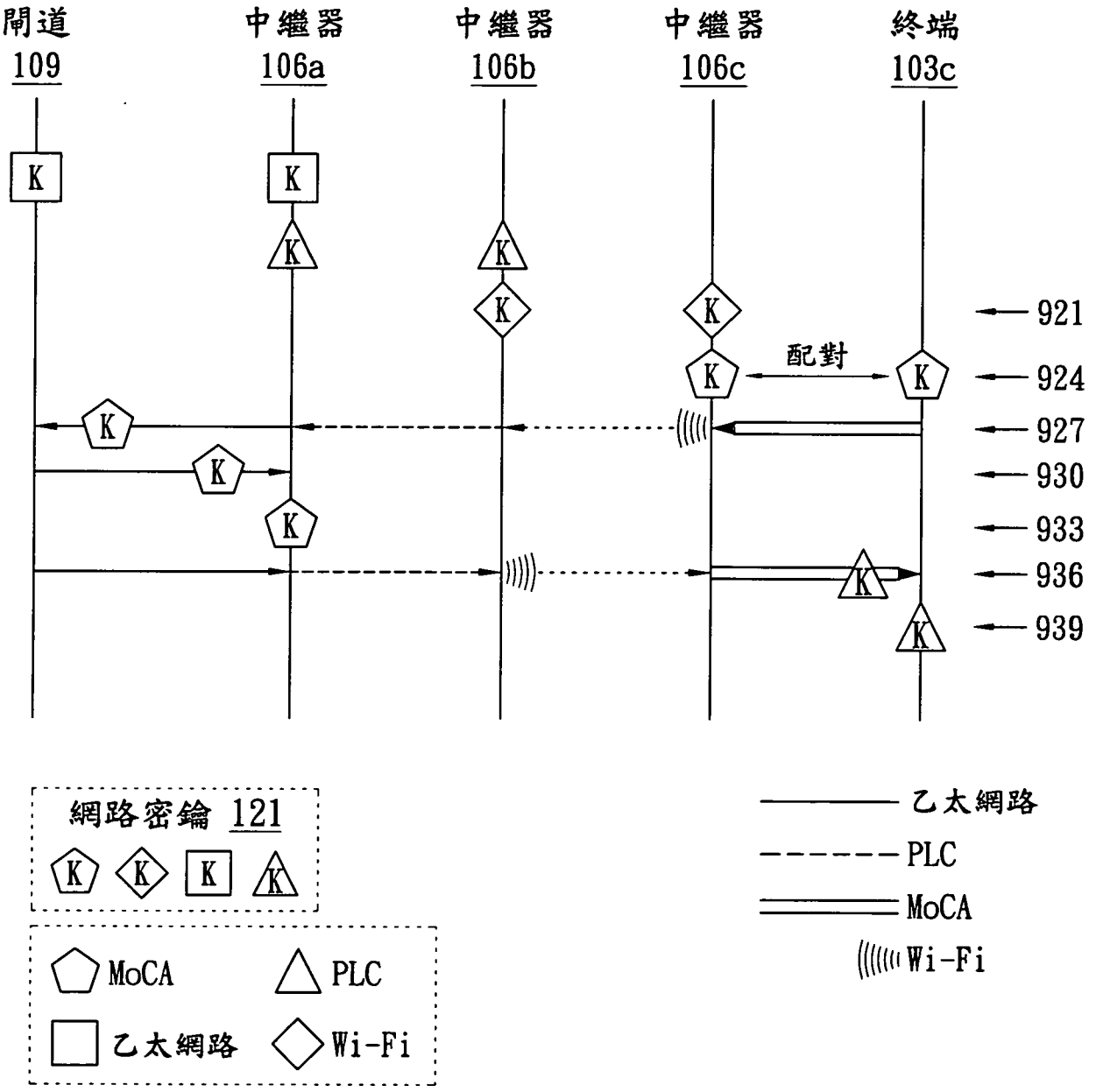
閘道
109
中繼器
106a
中繼器
106b
中繼器
106c
終端
103c
K
配對
921
924
927
930
933
936
939
網路密鑰 121
MoCA
PLC
乙太網路
Wi-Fi
乙太網路
PLC
MoCA
Wi-Fi

圖9C

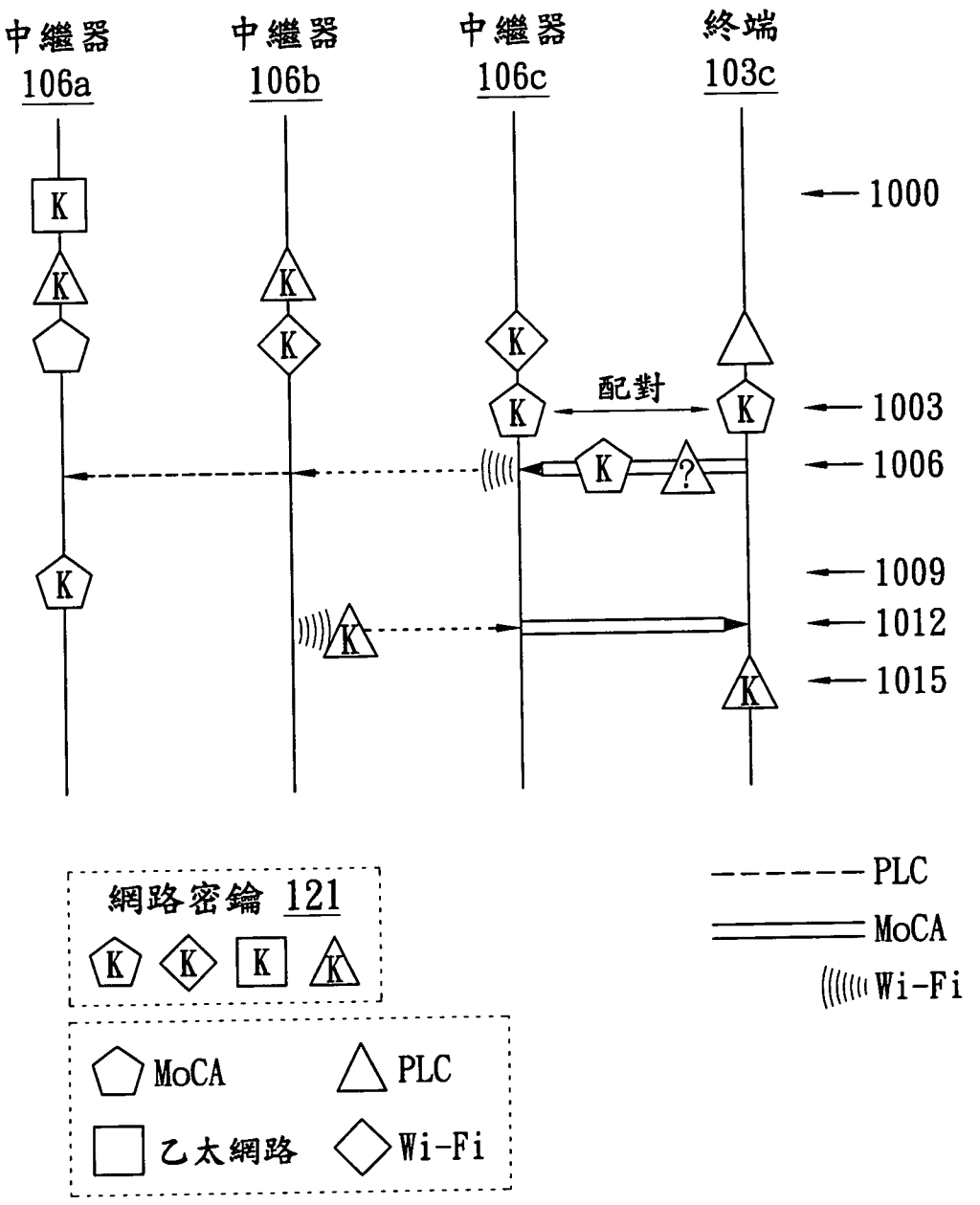
中繼器
106a
中繼器
106b
中繼器
106c
終端
103c
1000
配對
1003
1006
1009
1012
1015
網路密鑰 121
MoCA
PLC
乙太網路
Wi-Fi
PLC
MoCA
Wi-Fi

圖10

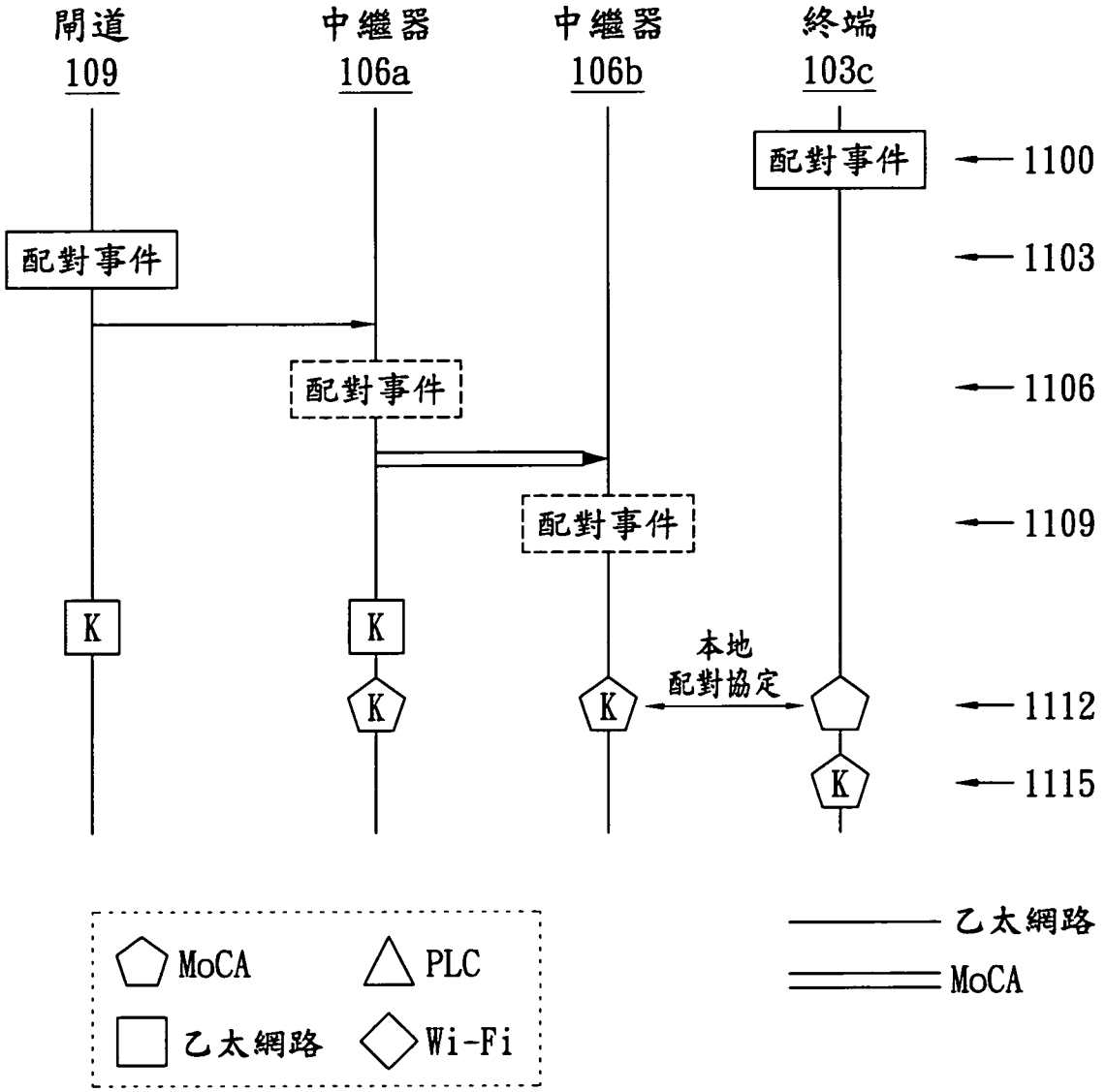
閘道
109
中繼器
106a
中繼器
106b
終端
103c
配對事件
1100
配對事件
1103
配對事件
1106
配對事件
1109
K
K
K
K
本地
配對協定
1112
K
1115
MoCA
PLC
乙太網路
Wi-Fi
乙太網路
MoCA

圖11