



(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 I698133 B

(45) 公告日：中華民國 109 (2020) 年 07 月 01 日

(21) 申請案號：107107394

(22) 申請日：中華民國 107 (2018) 年 03 月 06 日

(51) Int. Cl. : H04W12/06 (2009.01)

H04L29/06 (2006.01)

(30) 優先權：2017/06/28 中國大陸

201710506456.9

(71) 申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED (HK)

香港

(72) 發明人：王保初 (CN)

(74) 代理人：林志剛

(56) 參考文獻：

TW I254550

CN 104380776A

US 7107309B1

US 8316228B2

US 2008/0025278A1

US 2013/0040603A1

US 2013/0155876A1

US 2013/0166738A1

US 2016/0285841A1

審查人員：林東威

申請專利範圍項數：9 項 圖式數：4 共 33 頁

(54) 名稱

無線網路類型的檢測方法、裝置及電子設備

(57) 摘要

本發明提供一種無線網路類型的檢測方法、裝置及電子設備，所述方法包括：確定當前連接的無線網路在連接時是否需要密碼；在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。本發明實施例能夠準確地區分出無密碼連接的無線網路是否需要進行二次登錄驗證，從而能夠準確地向使用者提醒無線網路的安全風險，減小誤判率，減少對用戶的打擾。

指定代表圖：

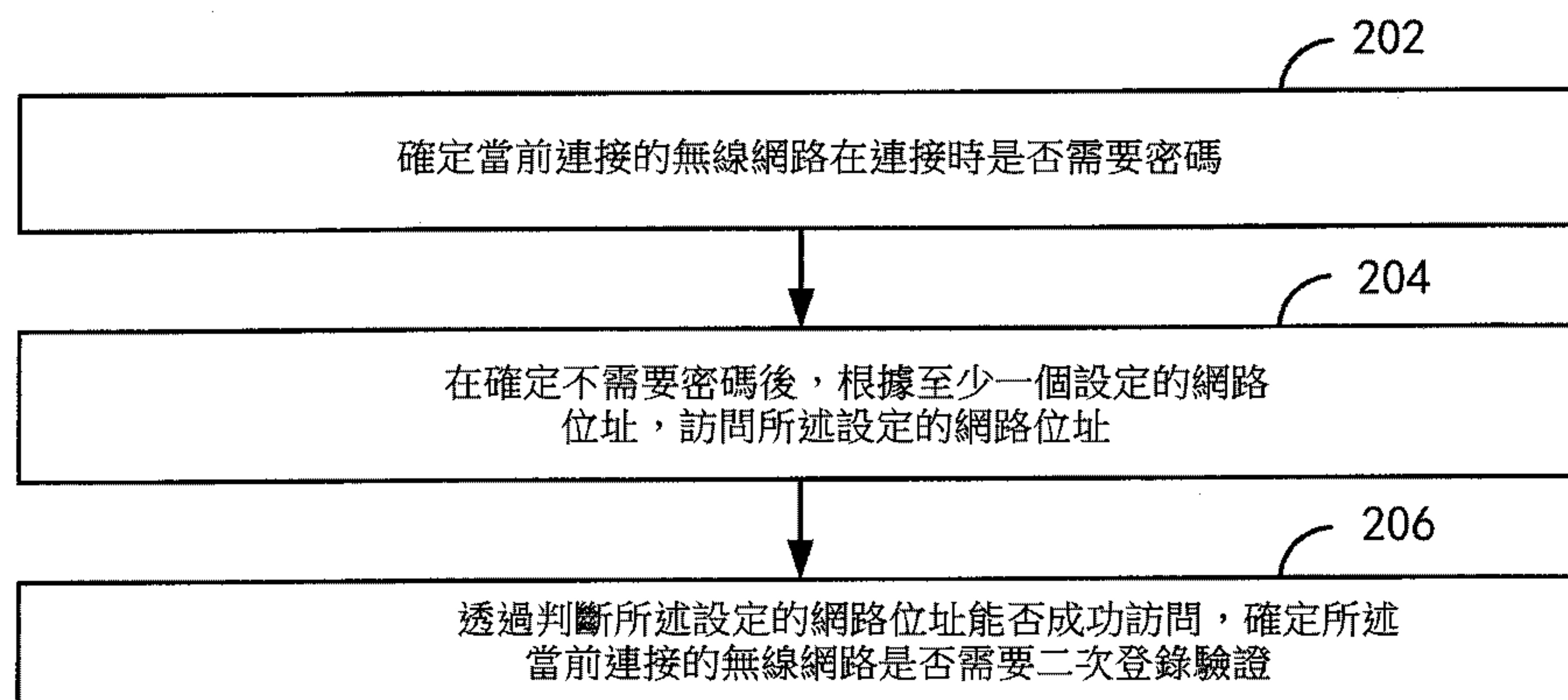


圖 2A



I698133

公告本

【發明摘要】

【中文發明名稱】

無線網路類型的檢測方法、裝置及電子設備

【中文】

本發明提供一種無線網路類型的檢測方法、裝置及電子設備，所述方法包括：確定當前連接的無線網路在連接時是否需要密碼；在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。本發明實施例能夠準確地區分出無密碼連接的無線網路是否需要進行二次登錄驗證，從而能夠準確地向使用者提醒無線網路的安全風險，減小誤判率，減少對用戶的打擾。

【指定代表圖】第(2A)圖。
【代表圖之符號簡單說明】無

【特徵化學式】無

【發明說明書】

【中文發明名稱】

無線網路類型的檢測方法、裝置及電子設備

【技術領域】

本發明涉及通信技術領域，尤其涉及無線網路類型的檢測方法、裝置及電子設備。

【先前技術】

隨著移動網際網路的發展，電子設備透過WiFi接入無線網路變得越來越頻繁，但與此同時，WiFi安全問題也越來越突出。電子設備可能會連接不安全的WiFi熱點，從而導致個人資訊洩漏、密碼洩漏或帳戶被盜等情況。

由於大多數不安全的WiFi熱點都不會設置登錄密碼，目的是為了方便使用者連接，使得更多的用戶接入不安全的WiFi熱點。因此，目前有較多安全工具類的應用程式，會在電子設備連接WiFi後，檢測當前WiFi是否需要密碼連接，如果是無密碼連接，則會阻止接入該WiFi熱點，或者給出安全提示。然而，某些無密碼的WiFi連接後，還需要使用者進行二次登錄驗證(二次登錄驗證是指，設備在連接WiFi熱點的時候並不需要密碼，但是在訪問網路的時候會彈出一個登錄介面，需要使用者輸入用戶名和密碼才能上網)。

【發明內容】

基於此，本發明提供了無線網路類型的檢測方法、裝置及電子設備。

一種無線網路類型的檢測方法，包括：

確定當前連接的無線網路在連接時是否需要密碼；

在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；

透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。

可選的，所述確定當前連接的無線網路在連接時是否需要密碼，包括：

調用作業系統提供的無線網路密碼管理介面，獲取調用結果，根據所述調用結果確定當前連接的無線網路在連接時是否需要密碼。

可選的，所述設定的網路位址包括自訂API介面的網路位址，所述API介面用於在被訪問時返回設定標識資訊；

所述判斷所述設定的網路位址能否成功訪問，包括：

獲取訪問所述API介面的網路位址後的訪問結果，根據所述訪問結果中是否包括所述設定標識資訊，確定所述API介面的網路位址能否成功訪問。

可選的，所述設定的網路位址至少包括有兩個不同的網頁的網路位址；

所述判斷所述設定的網路位址能否成功訪問，包括：

獲取訪問每個所述網頁的網路位址後返回的網頁的頁面資料，透過比較各所述網頁的頁面資料，判斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，進而確定各個所述網頁的網路位址能否成功訪問。

可選的，所述網頁的頁面資料包括有該網頁的網路位址；

所述透過比較各所述網頁的頁面資料，判斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，包括：

更新每個所述網頁的頁面資料，所述更新包括將每個所述網頁的頁面資料中包含的網路位址都刪除，或者都替換為統一標識資料；

比較各個所述網頁的更新後的頁面資料是否相同，根據比較結果確定訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面。

一種無線網路類型的檢測裝置，包括：

連接密碼確定模組，用於：確定當前連接的無線網路在連接時是否需要密碼；

訪問模組，用於：在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；

登錄驗證模組，用於：透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。

可選的，所述連接密碼確定模組，還用於：

調用作業系統提供的無線網路密碼管理介面，獲取調

用結果，根據所述調用結果確定當前連接的無線網路在連接時是否需要密碼。

可選的，所述設定的網路位址包括自訂API介面的網路位址，所述API介面用於在被訪問時返回設定標識資訊；

所述登錄驗證模組，還用於：

獲取訪問所述API介面的網路位址後的訪問結果，根據所述訪問結果中是否包括所述設定標識資訊，確定所述API介面的網路位址能否成功訪問。

可選的，所述設定的網路位址至少包括有兩個不同的網頁的網路位址；

所述登錄驗證模組，還用於：

獲取訪問每個所述網頁的網路位址後返回的網頁的頁面資料，透過比較各所述網頁的頁面資料，判斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，進而確定各個所述網頁的網路位址能否成功訪問。

可選的，所述網頁的頁面資料包括有該網頁的網路位址；

所述登錄驗證模組，還用於：

更新每個所述網頁的頁面資料，所述更新包括將每個所述網頁的頁面資料中包含的網路位址都刪除，或者都替換為統一標識資料；

比較各個所述網頁的更新後的頁面資料是否相同，根據比較結果確定訪問每個所述網頁後是否都跳轉至二次登

錄驗證頁面。

一種電子設備，包括：

處理器；

用於儲存處理器可執行指令的記憶體；

其中，所述處理器被配置為：

確定當前連接的無線網路在連接時是否需要密碼；

在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；

透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。

本發明的實施例提供的技術方案可以包括以下有益效果：

本發明的無線網路類型的檢測方法，在確定當前連接的無線網路在連接時不需要密碼後，進一步會訪問所設定的網路位址，透過判斷設定的網路位址能否成功訪問，若能夠成功訪問，可確定所述當前連接的無線網路為無密碼無線網路，若無法成功訪問，則確定為需要二次登錄驗證的無線網路。本發明實施例能夠準確無誤地區分出無密碼連接無線網路是否需要進行二次登錄驗證，能夠準確地向使用者提醒無線網路的安全風險，減小誤判率，減少對用戶的打擾。

應當理解的是，以上的一般描述和後文的細節描述僅是示例性和解釋性的，並不能限制本發明。

【圖式簡單說明】

此處的圖式被併入說明書中並構成本發明的一部分，示出了符合本發明的實施例，並與說明書一起用於解釋本發明的原理。

圖1是本發明根據一示例性實施例示出的一種電子設備透過WiFi連接無線網路的示意圖。

圖2A是本發明根據一示例性實施例示出的一種無線網路類型的檢測方法的流程圖。

圖2B是本發明根據一示例性實施例示出的一種電子設備中無線網路類型的檢測方案示意圖。

圖2C是本發明根據一示例性實施例示出的一種無線網路類型的檢測方法的流程圖。

圖2D是本發明根據一示例性實施例示出的一種無線網路類型的檢測方法的流程圖。

圖3是本發明無線網路類型的檢測裝置所在電子設備的一種硬體結構圖。

圖4是本發明根據一示例性實施例示出的一種無線網路類型的檢測裝置的方塊圖。

【實施方式】

這裡將詳細地對示例性實施例進行說明，其示例表示在圖式中。下面的描述涉及圖式時，除非另有表示，不同圖式中的相同數字表示相同或相似的要素。以下示例性實施例中所描述的實施方式並不代表與本發明相一致的所有

實施方式。相反，它們僅是與如申請專利範圍中所詳述的、本發明的一些方面相一致的裝置和方法的例子。

在本發明使用的術語是僅僅出於描述特定實施例的目的，而非旨在限制本發明。在本發明和申請專利範圍中所使用的單數形式的“一種”、“所述”和“該”也旨在包括多數形式，除非上下文清楚地表示其他含義。還應當理解，本文中使用的術語“和/或”是指並包含一個或多個相關聯的列出專案的任何或所有可能組合。

應當理解，儘管在本發明可能採用術語第一、第二、第三等來描述各種資訊，但這些資訊不應限於這些術語。這些術語僅用來將同一類型的資訊彼此區分開。例如，在不脫離本發明範圍的情況下，第一資訊也可以被稱為第二資訊，類似地，第二資訊也可以被稱為第一資訊。取決於語境，如在此所使用的詞語“如果”可以被解釋成為“在……時”或“當……時”或“回應於確定”。

本發明實施例中，WiFi是一種允許電子設備連接到一個無線區域網(WLAN, Wireless LAN)的技術，可以將個人電腦、手持設備(如PDA、手機)等終端以無線方式互相連接。

WiFi熱點是指能夠提供共用網路資源，讓其它終端(如手機、筆記型電腦)透過WiFi連接方式進行聯網的設備。例如一個無線路由器，在這個無線路由器的電波覆蓋的有效範圍都可以採用WiFi連接方式進行無線網路互連，這台無線路由器就被稱為一個“WiFi熱點”。

WiFi二次登錄驗證：設備在連接**WiFi**熱點的時候並不需要密碼，但是在訪問網路的時候會彈出一個登錄介面，需要使用者輸入用戶名和密碼才能上網。這種登錄連接方式稱之為“**WiFi二次登錄驗證**”。

如圖1所示，是本發明根據一示例性實施例示出的一種電子設備透過**WiFi**連接無線網路的示意圖，電子設備在連接一無線網路熱點時不需要密碼即可加入該無線網路，但是，該無線網路在訪問**Internet**時需要二次登錄驗證，需要使用者輸入帳號和密碼，因此並不是實際意義上的無密碼**WiFi**。

本發明實施例的無線網路類型的檢測方案，在確定當前連接的無線網路在連接時不需要密碼後，進一步可以訪問所設定的網路位址，透過判斷設定的網路位址能否成功訪問，若能夠成功訪問，可確定所述當前連接的無線網路為無密碼無線網路，若無法成功訪問，則確定為需要二次登錄驗證的無線網路。本發明實施例能夠準確無誤地區分出無密碼連接無線網路是否需要進行二次登錄驗證，能夠準確地向使用者提醒無線網路的安全風險，減小誤判率，減少對用戶的打擾。接下來對本發明實施例進行詳細說明。

如圖2A所示，圖2A是本發明根據一示例性實施例示出的一種無線網路類型的檢測方法的流程圖，包括以下步驟202至206：

在步驟202中，確定當前連接的無線網路在連接時是

否需要密碼。

在步驟 204 中，在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址。

在步驟 206 中，透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。

本實施例中的方法可應用於配置有無線網路模組的電子設備中，例如可以是應用於安裝在電子設備的應用程式，該應用程式能檢測電子設備所接入的無線網路的類型，以根據所檢測的類型向使用者提供針對無線網路的安全風險提示。本實施例的電子設備可以包括智慧手機、平板電腦、個人數位助理或多媒體播放機等等，此類電子設備配置有無線網路模組，能夠接入無線網路。如圖 2B 所示，是本發明根據一示例性實施例示出的一種電子設備中無線網路類型的檢測方案示意圖。

當電子設備在連接路由器、閘道設備或其他網路終端提供的無線網路，應用程式可以透過多種方式確定電子設備連接上無線網路，並且是否需要密碼接入。例如，在應用程式具備許可權的情況下，可以直接與無線網路模組通信、或者是讀取無線網路模組提供的介面等方式確定電子設備接入了無線網路 WiFi 熱點，並確定所接入的無線網路 WiFi 熱點在連接時是否需要密碼；在其他例子中，應用程式可能具備許可權，而電子設備的作業系統提供有介面，可以透過調用介面後的調用結果進行判斷。實際應用中，

可以根據電子設備所使用的作業系統、應用程式的廠商所能得到的作業系統的許可權、以及作業系統所提供的介面等等多種因素而靈活確定。

在一個可選的實現方式中，所述確定當前連接的無線網路在連接時是否需要密碼，可以包括：

調用作業系統提供的無線網路密碼管理介面，獲取調用結果，根據所述調用結果確定當前連接的無線網路在連接時是否需要密碼。

以安卓(Android)作業系統為例，作業系統提供有針對無線網路模組的無線網路密碼管理介面，應用程式可調用該介面，透過調用該介面的調用結果，可以確定當前連接的無線網路在連接時是否需要密碼。以下示出了一種調用無線網路管理介面的代碼：

```

/**
 * 利用 WiFiConfiguration.KeyMgmt 的管理機制，來判斷當前連接的
WiFi 在接入是否需要密碼
 *
 * @return true: 需要密碼連接, false: 不需要密碼連接
 */
public static boolean needPassword(Context context) {
    WiFiManager          WiFiManager          =          (WiFiManager)

```

```

context.getSystemService(Context.WiFi_SERVICE);
    if (WifiManager != null) {
        List<WifiConfiguration> wifiConfigurationList =
WifiManager.getConfiguredNetworks();
        if (wifiConfigurationList != null && wifiConfigurationList.size() > 0)
        {
            for (WifiConfiguration configuration : wifiConfigurationList)
            {
                if (configuration != null && configuration.status ==
WifiConfiguration.Status.CURRENT) {
                    if
(configuration.allowedKeyManagement.get(WifiConfiguration.KeyMgmt.NONE)) {
                        return false;
                    } else {
                        return true;
                    }
                }
            }
        }
        // 預設為需要連接密碼
        return true;
    }
}

```

其中，`WifiManager.getConfiguredNetworks()`表示無線網路密碼管理介面，該代碼的主要邏輯是檢測：

WiFi熱點的`WifiConfiguration.allowedKeyManagement`是否包含`WifiConfiguration.KeyMgmt.NONE`欄位。如果包含，則認為不需要密碼，否則認為需要密碼。在不需要密

碼連接無線網路時，調用結果中會包含有 `KeyMgmt.NONE` 欄位。

以 iOS 作業系統為例，iOS 作業系統提供了獲取 WiFi 清單的 API (介面名稱為 `NEHotspotNetwork`)，主要步驟有：向 Apple 申請開發 `Network Extension` 許可權、申請包含 `Network Extension` 的描述檔、配置 `Info.plist`、配置 `entitlements`、iOS 獲取 WiFi 列表代碼實現、獲取 WiFi 列表回檔。

在調用 `NEHotspotNetwork` 後，`NEHotspotNetwork` 返回的資訊包括有：

`SSID`：WiFi 名稱

`BSSID`：網站的 MAC 地址

`signalStrength`：WiFi 信號強度，該值在 0.0-1.0 之間

`secure`：網路是否安全（不需要密碼接入的 WiFi，該值為 `false`）

`autoJoined`：設備是否自動連接該 WiFi。

`justJoined`：網路是否剛剛加入

`chosenHelper`：`HotspotHelper` 是否為網路的所選助手

因此，透過調用結果中的 `secure`，即可確定當前連接的無線網路 WiFi 熱點是否需要密碼。

然而，無密碼接入無線網路時，某些無線網路還需要使用者二次登錄驗證。因此，本實施例透過預先設定一個或多個網路位址，並透過訪問設定的網路位址的方式判斷是否需要二次登錄驗證。假設需要二次登錄驗證，則還需

要使用者輸入帳戶和密碼之後才可訪問 Internet。若使用者未進行二次登錄驗證，在電子設備在訪問 Internet 後，無法獲得需要的網路資料。基於此，本實施例設定有一個或多個網路位址，訪問設定的網路位址後，若能成功訪問，則表示所接入的無線網路不需要進行二次登錄驗證，若不能成功訪問，則表示所接入的無線網路需要進行二次登錄驗證。

對於如何確定是否成功訪問，實際應用中可以有多種方式。例如，對於設定的網路位址，可以預先配置對應的網路位址的網路資料，在訪問設定的網路位址後，獲取訪問結果，根據訪問結果與預先配置的網路資料是否相同，進而確定是否能夠成功訪問。

本實施例中，所述設定的網路位址包括自訂 API 介面的網路位址，所述 API 介面用於在被訪問時返回設定標識資訊。

所述判斷所述設定的網路位址能否成功訪問，包括：
獲取訪問所述 API 介面的網路位址後的訪問結果，根據所述訪問結果中是否包括所述設定標識資訊，確定所述 API 介面的網路位址能否成功訪問。

本實施例中可以預先在伺服器開發有 API 介面，應用程式可以訪問 API 介面的網路位址，該網路位址可以是指 IP 位址。若網路能通，則訪問 API 介面後可以獲得該設定標識資訊，若網路不通，則無法獲得該設定標識資訊，從而可以確定所述 API 介面的網路位址能否成功訪問，確定

是否需要二次登錄驗證。

在另一些例子中，還可以不進行預先開發的工作，網路位址可以是公共的網頁的網路位址，可以預先分析該網頁的頁面內容並儲存，確定訪問該網頁後的訪問結果是否包括上述預先儲存的頁面內容，進而確定是否成功訪問。然而，網頁頁面內容可能會動態變化，因此，本實施例可以設定兩個以上的網頁的網路位址，以提供更為可靠的判斷方式，具體的，本發明提供如下實施例：

所述設定的網路位址至少包括兩個不同的網頁的網路位址。

所述判斷所述設定的網路位址能否成功訪問，包括：

獲取訪問每個所述網頁的網路位址後返回的網頁的頁面資料，透過比較各所述網頁的頁面資料，判斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，進而確定所述網頁的網路位址能否成功訪問。

其中，上述網頁可以選取已有的兩個或兩個以上的公共網頁，並可以選取頁面內容較為簡單的網頁，以減少資料流程量消耗。該網路位址可以包括網頁的功能變數名稱位址或者IP位址。假設網路不通，則訪問各個網頁後，都將跳轉至二次登錄驗證的網頁，則返回的都是二次登錄驗證的網頁的頁面資料，返回的頁面資料基本上都是相同的。若網路能通，則訪問兩個或兩個以上網頁後，返回的是各網頁的頁面資料，各網頁的頁面資料應該是不同的。因此，本實施例透過比較各所述網頁的頁面資料，能夠判

斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，進而確定各個所述網頁的網路位址能否成功訪問。

當向一個網路位址發起訪問後可獲得該網路位址返回的頁面資料，該頁面資料中包括有該網頁的網路位址，假設網路不同，返回的頁面資料包括有二次登錄驗證頁面的頁面資料，則除了網路位址之外，其他的頁面資料都是相同的。基於此，為了提高判斷效率和判斷準確性，本實施例中，所述透過比較各所述網頁的頁面資料，判斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，包括：

更新每個所述網頁的頁面資料，所述更新包括將每個所述網頁的頁面資料中包含的網路位址都刪除，或者都替換為統一標識資料；

比較各個所述網頁的更新後的頁面資料是否相同，根據比較結果確定訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面。

本實施例中，將頁面資料中的網路位址刪除掉，或者是都替換為統一標識資料，之後再比較各個所述網頁的更新後的頁面資料是否相同，因此可以顯著提高比較效率和準確性。

接下來再透過兩個實施例詳細說明本發明。

如圖2C所示，是本發明根據一示例性實施例示出的一種無線網路類型的檢測方法的流程圖，圖2C以安卓作業系統為例，調用作業系統的無線網路密碼管理介面，即 `WiFiManager.getConfiguredNetworks()`，根據調用結果中

是否包括 `WiFiConfiguration.KeyMgmt.NONE` 欄位的基礎上進行判斷，如果不包含該欄位則認為需要密碼，立即返回判斷結果；如果包含該欄位，可以進一步判斷當前連接的無線網路 WiFi 熱點是否需要二次登錄驗證。

具體的，可以在自有伺服器上開發一個介面 API，該介面 API 的作用是需返回一個簡單的 `Success` 標誌即可。應用程式直接訪問該介面 API，如果能收到 `Success` 標誌，則認為當前連接的無線網路 WiFi 熱點可以直接上網，不需要進行二次登錄驗證；否則認為需要二次登錄驗證。

如圖 2D 所示，是本發明根據一示例性實施例示出的另一種無線網路類型的檢測方法的流程圖，圖 2D 以安卓作業系統為例，調用作業系統的無線網路密碼管理介面，即 `WiFiManager.getConfiguredNetworks()`，根據調用結果中是否包括 `WiFiConfiguration.KeyMgmt.NONE` 欄位的基礎上進行判斷，如果不包含該欄位則認為需要密碼，立即返回判斷結果；如果包含該欄位，可以進一步判斷當前連接的無線網路 WiFi 熱點是否需要二次登錄驗證。

具體的，相對於圖 2C 中在自有伺服器上開發 API 介面，本實施例可以選取兩個簡單的知名網地位址（網站頁面可以儘量簡單，以減少資料流程量消耗），假設為網站 A（網地位址為 `url_A`）和網站 B（網地位址為 `url_B`）；然後依次訪問網站 `url_A` 和網站 `url_B`，分別將它們返回的 `Response` 資料保存起來，對應記錄為 `response_A` 和 `response_B`；最後將 `response_A` 與 `response_B` 的內容進行

比較。

如果當前連接的無線網路WiFi熱點需要進行二次登錄驗證，則訪問網站url_A和網站url_B都會跳轉到二次登錄驗證頁面，即response_A與response_B的內容中包括了相同的二次登錄驗證頁面的頁面資料；否則response_A與response_B將代表不同網站的內容，肯定不同；由此可以判斷當前WiFi是否需二次登錄驗證。

然而，由於response_A與response_B中包括了對應的網路位址，在進行response_A與response_B對比之前，可以先將網路位址替換為統一標識資料。本實施例中都替換為url_B，因此可以執行response_A.replace(“url_A”, “url_B”)，即將response_A中的網址用url_B取代，消除網頁數據中不同網址的差異性，從而避免誤判，提高判斷效率和判斷準確性。

與前述無線網路類型的檢測方法的實施例相對應，本發明還提供了無線網路類型的檢測裝置及其所應用的電子設備的實施例。

本發明無線網路類型的檢測裝置的實施例可以應用在電子設備上。裝置實施例可以透過軟體實現，也可以透過硬體或者軟硬體結合的方式實現。以軟體實現為例，作為一個邏輯意義上的裝置，是透過其所在無線網路類型的檢測的處理器將非易失性記憶體中對應的電腦程式指令讀取到記憶體中運行形成的。從硬體層面而言，如圖3所示，為本發明無線網路類型的檢測裝置所在電子設備的一種硬

體結構圖，除了圖3所示的處理器310、記憶體330、網路介面320、以及非易失性記憶體340之外，實施例中裝置331所在的電子設備，通常根據該電腦設備的實際功能，還可以包括其他硬體，對此不再贅述。

如圖4所示，圖4是本發明根據一示例性實施例示出的一種無線網路類型的檢測裝置的方塊圖，所述裝置包括：

連接密碼確定模組41，用於：確定當前連接的無線網路在連接時是否需要密碼；

訪問模組42，用於：在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；

登錄驗證模組43，用於：透過判斷所述設定的網路位址能否成功訪問，確定所述當前連接的無線網路是否需要二次登錄驗證。

可選的，所述連接密碼確定模組，還用於：

調用作業系統提供的無線網路密碼管理介面，獲取調用結果，根據所述調用結果確定當前連接的無線網路在連接時是否需要密碼。

可選的，所述設定的網路位址包括自訂API介面的網路位址，所述API介面用於在被訪問時返回設定標識資訊；

所述登錄驗證模組，還用於：

獲取訪問所述API介面的網路位址後的訪問結果，根據所述訪問結果中是否包括所述設定標識資訊，確定所述API介面的網路位址能否成功訪問。

可選的，所述設定的網路位址至少包括有兩個不同的網頁的網路位址；

所述登錄驗證模組，還用於：

獲取訪問每個所述網頁的網路位址後返回的網頁的頁面資料，透過比較各所述網頁的頁面資料，判斷訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面，進而確定各個所述網頁的網路位址能否成功訪問。

可選的，所述網頁的頁面資料包括有該網頁的網路位址；

所述登錄驗證模組，還用於：

更新每個所述網頁的頁面資料，所述更新包括將每個所述網頁的頁面資料中包含的網路位址都刪除，或者都替換為統一標識資料；

比較各個所述網頁的更新後的頁面資料是否相同，根據比較結果確定訪問每個所述網頁後是否都跳轉至二次登錄驗證頁面。

一種電子設備，包括：

處理器；

用於儲存處理器可執行指令的記憶體；

其中，所述處理器被配置為：

確定當前連接的無線網路在連接時是否需要密碼；

在確定不需要密碼後，根據至少一個設定的網路位址，訪問所述設定的網路位址；

透過判斷所述設定的網路位址能否成功訪問，確定所

述當前連接的無線網路是否需要二次登錄驗證。

上述裝置中各個模組的功能和作用的實現過程具體詳見上述方法中對應步驟的實現過程，在此不再贅述。

對於裝置實施例而言，由於其基本對應於方法實施例，所以相關之處參見方法實施例的部分說明即可。以上所描述的裝置實施例僅僅是示意性的，其中所述作為分離部件說明的模組可以是或者也可以不是實體上分開的，作為模組顯示的部件可以是或者也可以不是實體模組，即可以位於一個地方，或者也可以分佈到多個網路模組上。可以根據實際的需要選擇其中的部分或者全部模組來實現本發明方案的目的。本領域普通技術人員在不付出創造性勞動的情況下，即可以理解並實施。

上述對本發明特定實施例進行了描述。其它實施例在申請專利範圍的範圍內。在一些情況下，在申請專利範圍中記載的動作或步驟可以按照不同於實施例中的順序來執行並且仍然可以實現期望的結果。另外，在圖式中描繪的過程不一定要求示出的特定順序或者連續順序才能實現期望的結果。在某些實施方式中，多工處理和並行處理也是可以的或者可能是有利的。

本領域技術人員在考慮說明書及實踐這裡申請的發明後，將容易想到本發明的其它實施方案。本發明旨在涵蓋本發明的任何變型、用途或者適應性變化，這些變型、用途或者適應性變化遵循本發明的一般性原理並包括本發明未申請的本技術領域中的公知常識或慣用技術手段。說明

書和實施例僅被視為示例性的，本發明的真正範圍和精神由申請專利範圍指出。

應當理解的是，本發明並不局限於上面已經描述並在圖式中示出的精確結構，並且可以在不脫離其範圍進行各種修改和改變。本發明的範圍僅由申請專利範圍來限制。

以上所述僅為本發明的較佳實施例而已，並不用以限制本發明，凡在本發明的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本發明保護的範圍之內。

【符號說明】

41：連接密碼確定模組

42：訪問模組

43：登錄驗證模組

310：處理器

320：網路介面

330：記憶體

331：無線網路類型的檢測裝置

340：非易失性記憶體

【發明申請專利範圍】

【第1項】

一種無線網路類型的檢測方法，包括：

確定當前連接的無線網路在連接時是否需要密碼；

在確定當前連接的該無線網路在連接時不需要密碼後，透過該無線網路，從關聯於不同網頁的至少兩個網路位址來檢索資料；

至少根據下列步驟來確定該當前連接的無線網路在連接時是否需要二次登錄驗證：

訪問關聯於不同網頁的該至少兩個網路位址的每一個網路位址；

針對每一個被訪問的網路位址，獲取包含關聯於該至少兩個網路位址其中一個的第一網頁頁面資料以及關聯於該至少兩個網路位址其中不同的一個的第二網頁頁面資料的網頁頁面資料；

比較該第一網頁頁面資料與該第二網頁頁面資料，以確定該第一網頁頁面資料是否匹配該第二網頁頁面資料；以及

在確定該第一網頁頁面資料匹配該第二網頁頁面資料後，確定當前連接的該無線網路在連接時需要二次登錄驗證。

【第2項】

根據申請專利範圍第1項的方法，該確定當前連接的無線網路在連接時是否需要密碼，包括：

調用作業系統提供的無線網路密碼管理介面，獲取調用結果，根據該調用結果確定當前連接的無線網路在連接時是否需要密碼。

【第3項】

根據申請專利範圍第1項的方法，該網路位址包括自訂API介面的網路位址，該API介面用於在被訪問時返回設定標識資訊；

該判斷該網路位址能否成功訪問，包括：

獲取訪問該API介面的網路位址後的訪問結果，根據該訪問結果中是否包括該設定標識資訊，確定該API介面的網路位址能否成功訪問。

【第4項】

根據申請專利範圍第1項的方法，該比較該第一網頁頁面資料與該第二網頁頁面資料，包括：

更新該第一網頁頁面資料與該第二網頁頁面資料，該更新包括將該第一網頁頁面資料與該第二網頁頁面資料中包含的網路位址都刪除，或者都替換為統一標識資料；

比較更新後的第一網頁頁面資料與更新後的第二網頁頁面資料。

【第5項】

一種無線網路類型的檢測裝置，包括：

連接密碼確定模組，用於：確定當前連接的無線網路在連接時是否需要密碼；

訪問模組，用於：在確定當前連接的該無線網路在連

接時不需要密碼後，透過該無線網路，從關聯於不同網頁的至少兩個網路位址來檢索資料；

登錄驗證模組，用於：至少根據下列步驟來確定該當前連接的無線網路在連接時是否需要二次登錄驗證：

訪問關聯於不同網頁的該至少兩個網路位址的每一個網路位址；

針對每一個被訪問的網路位址，獲取包含關聯於該至少兩個網路位址其中一個的第一網頁頁面資料以及關聯於該至少兩個網路位址其中不同的一個的第二網頁頁面資料的網頁頁面資料；

比較該第一網頁頁面資料與該第二網頁頁面資料，以確定該第一網頁頁面資料是否匹配該第二網頁頁面資料；以及

在確定該第一網頁頁面資料匹配該第二網頁頁面資料後，確定當前連接的該無線網路在連接時需要二次登錄驗證。

【第6項】

根據申請專利範圍第5項的裝置，該連接密碼確定模組，還用於：

調用作業系統提供的無線網路密碼管理介面，獲取調用結果，根據該調用結果確定當前連接的無線網路在連接時是否需要密碼。

【第7項】

根據申請專利範圍第5項的裝置，該網路位址包括自

訂 API 介面的網路位址，該 API 介面用於在被訪問時返回設定標識資訊；

該登錄驗證模組，還用於：

獲取訪問該 API 介面的網路位址後的訪問結果，根據該訪問結果中是否包括該設定標識資訊，確定該 API 介面的網路位址能否成功訪問。

【第 8 項】

根據申請專利範圍第 5 項的裝置，

該登錄驗證模組，還用於：

更新該第一網頁頁面資料與該第二網頁頁面資料，該更新包括將該第一網頁頁面資料與該第二網頁頁面資料中包含的網路位址都刪除，或者都替換為統一標識資料；

比較更新後的第一網頁頁面資料與更新後的第二網頁頁面資料。

【第 9 項】

一種電子設備，包括：

處理器；

用於儲存處理器可執行指令的記憶體；

其中，該處理器被配置為：

確定當前連接的無線網路在連接時是否需要密碼；

在確定當前連接的該無線網路在連接時不需要密碼後，透過該無線網路，從關聯於不同網頁的至少兩個網路位址來檢索資料；

至少根據下列步驟來確定該當前連接的無線網路在連

接時是否需要二次登錄驗證：

訪問關聯於不同網頁的該至少兩個網路位址的每一個網路位址；

針對每一個被訪問的網路位址，獲取包含關聯於該至少兩個網路位址其中一個的第一網頁頁面資料以及關聯於該至少兩個網路位址其中不同的一個的第二網頁頁面資料的網頁頁面資料；

比較該第一網頁頁面資料與該第二網頁頁面資料，以確定該第一網頁頁面資料是否匹配該第二網頁頁面資料；以及

在確定該第一網頁頁面資料匹配該第二網頁頁面資料後，確定當前連接的該無線網路在連接時需要二次登錄驗證。

【發明圖式】

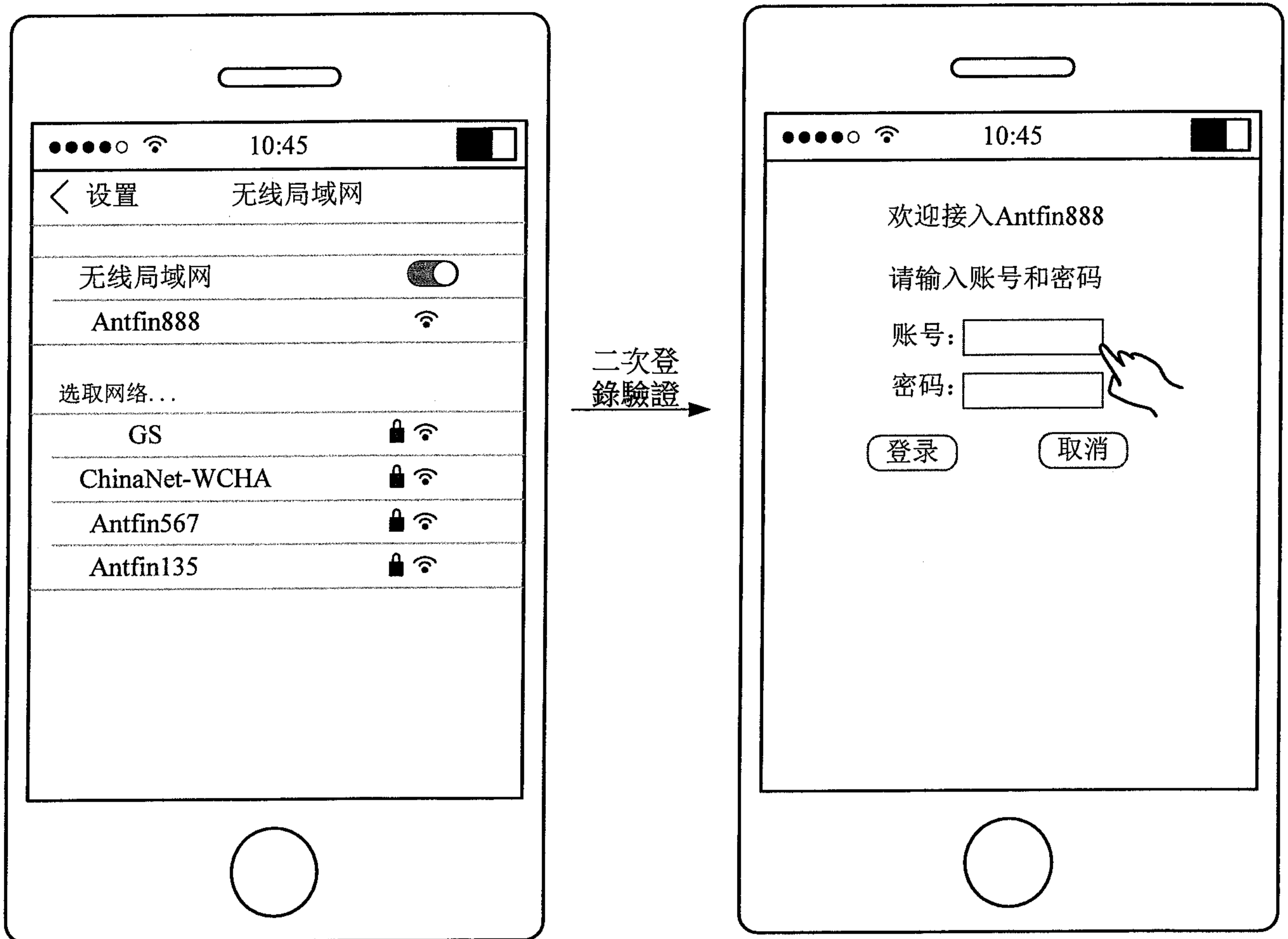


圖 1

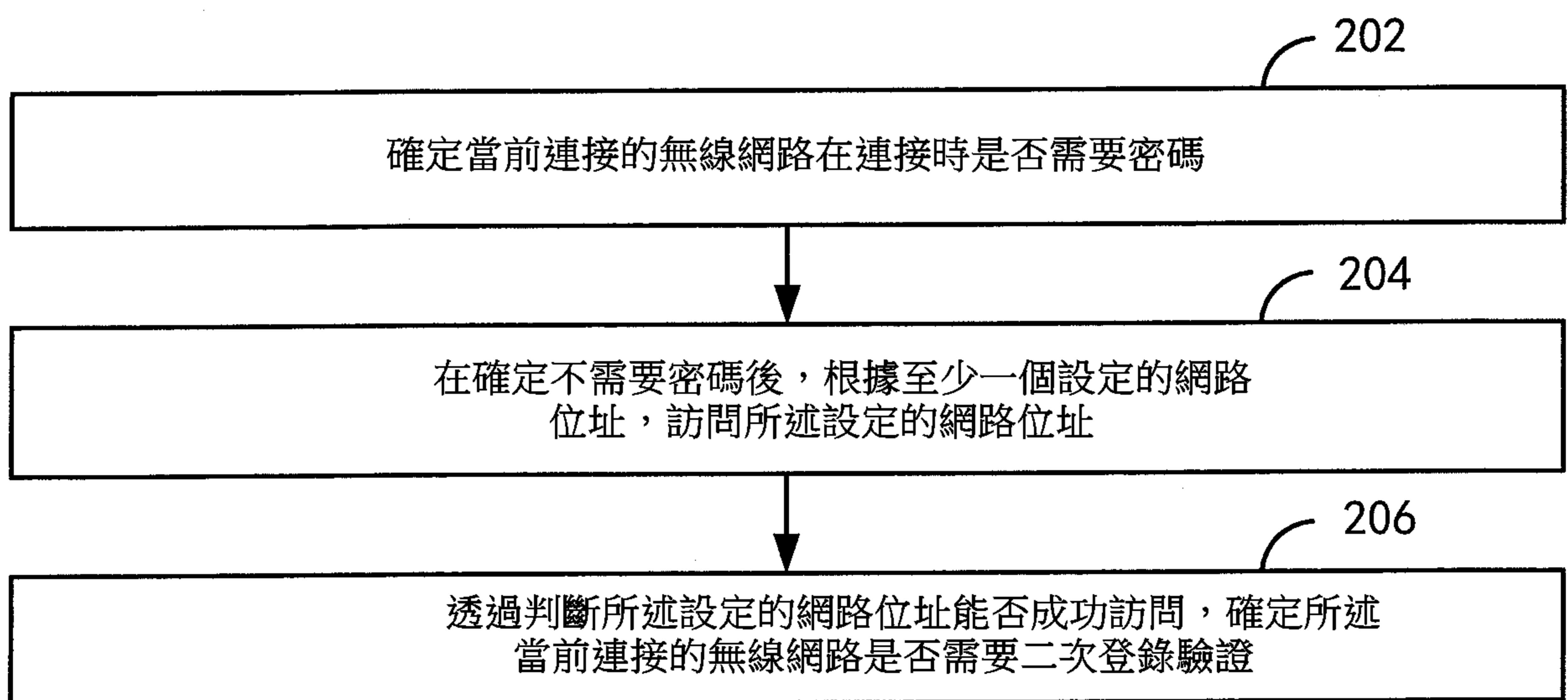


圖 2A

確定不需要密碼後，後臺訪問設定的網路位址，判斷能否成功訪問，進而確定是否需要二次登錄驗證

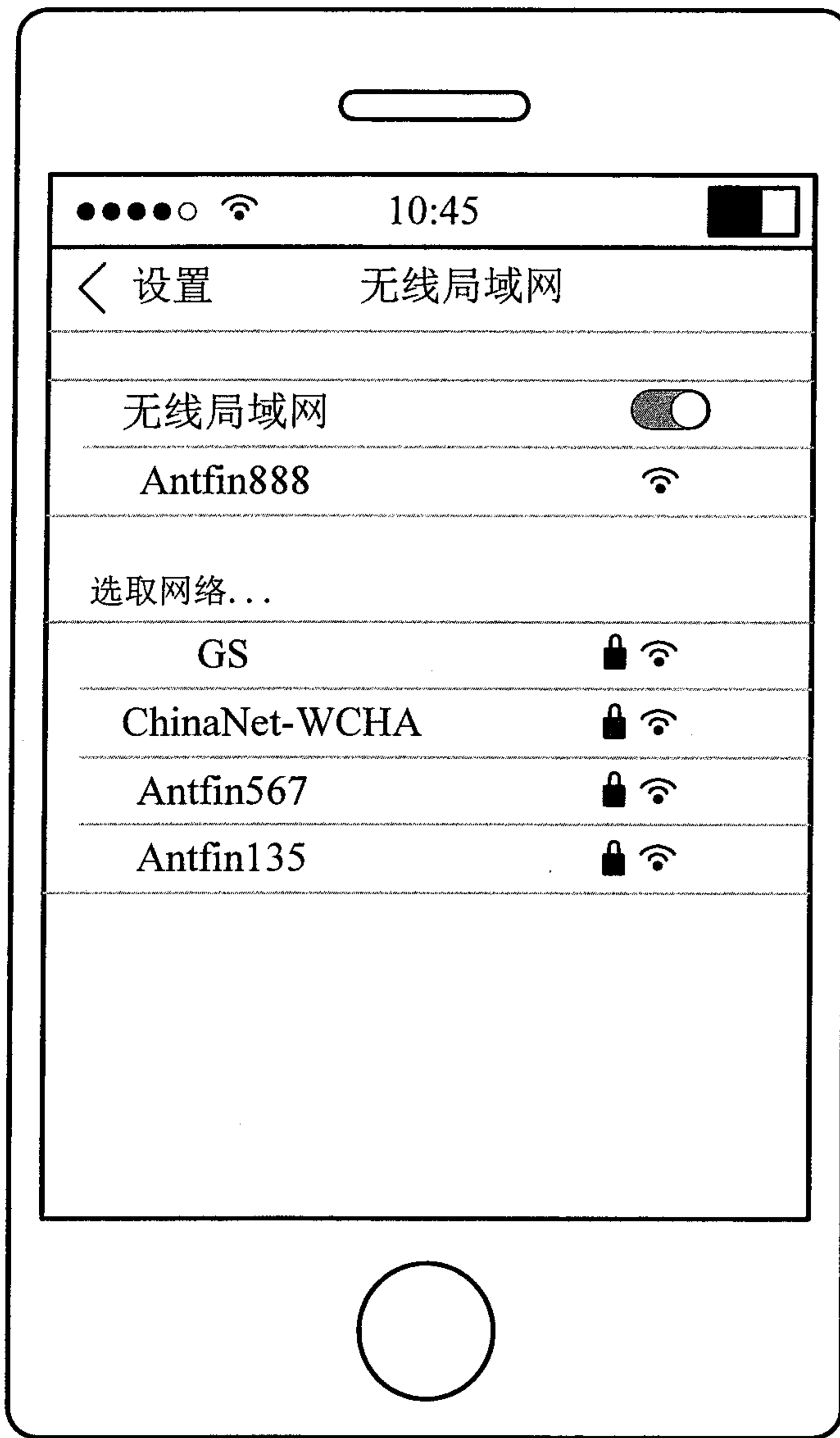


圖 2B

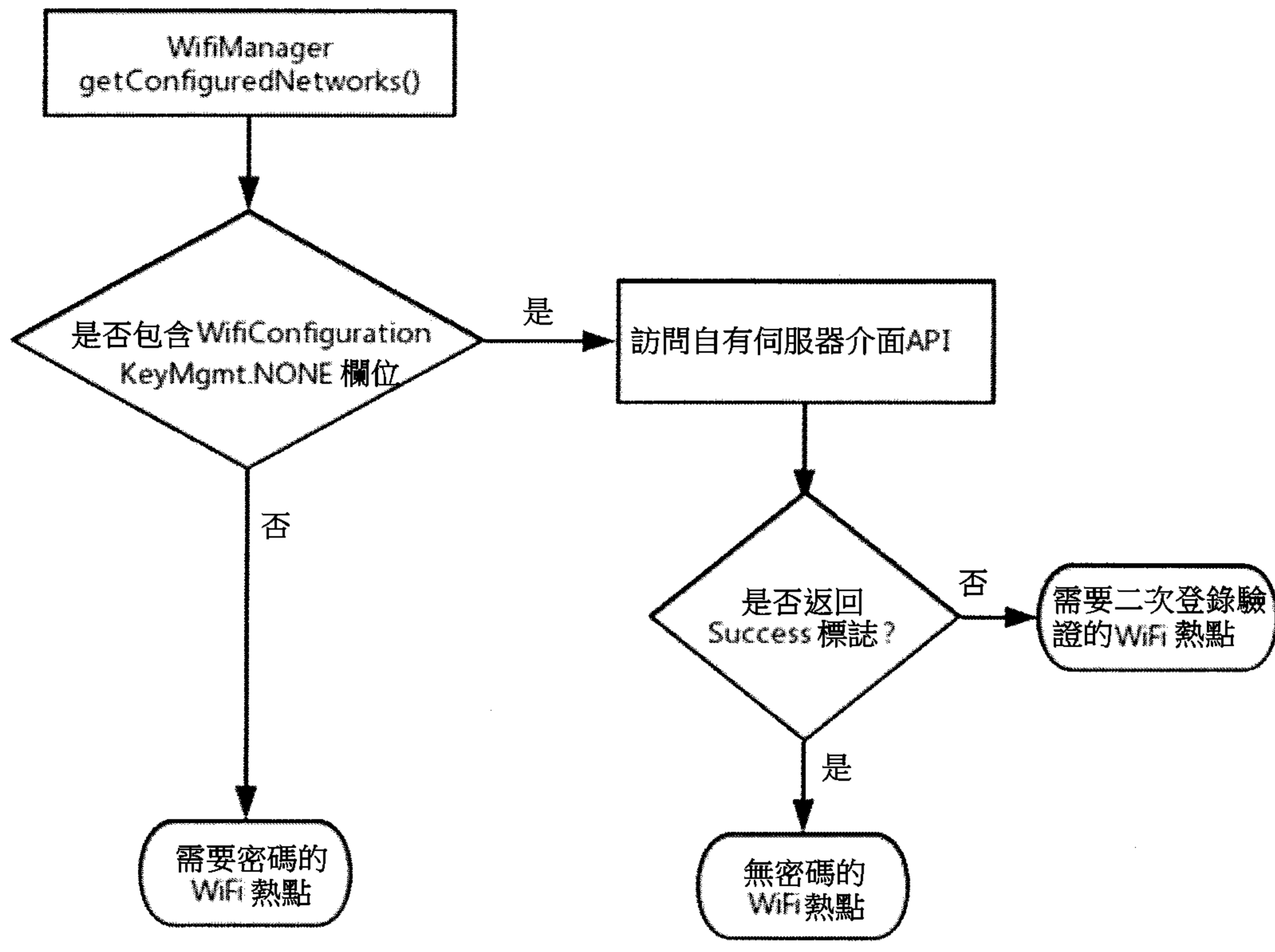


圖 2C

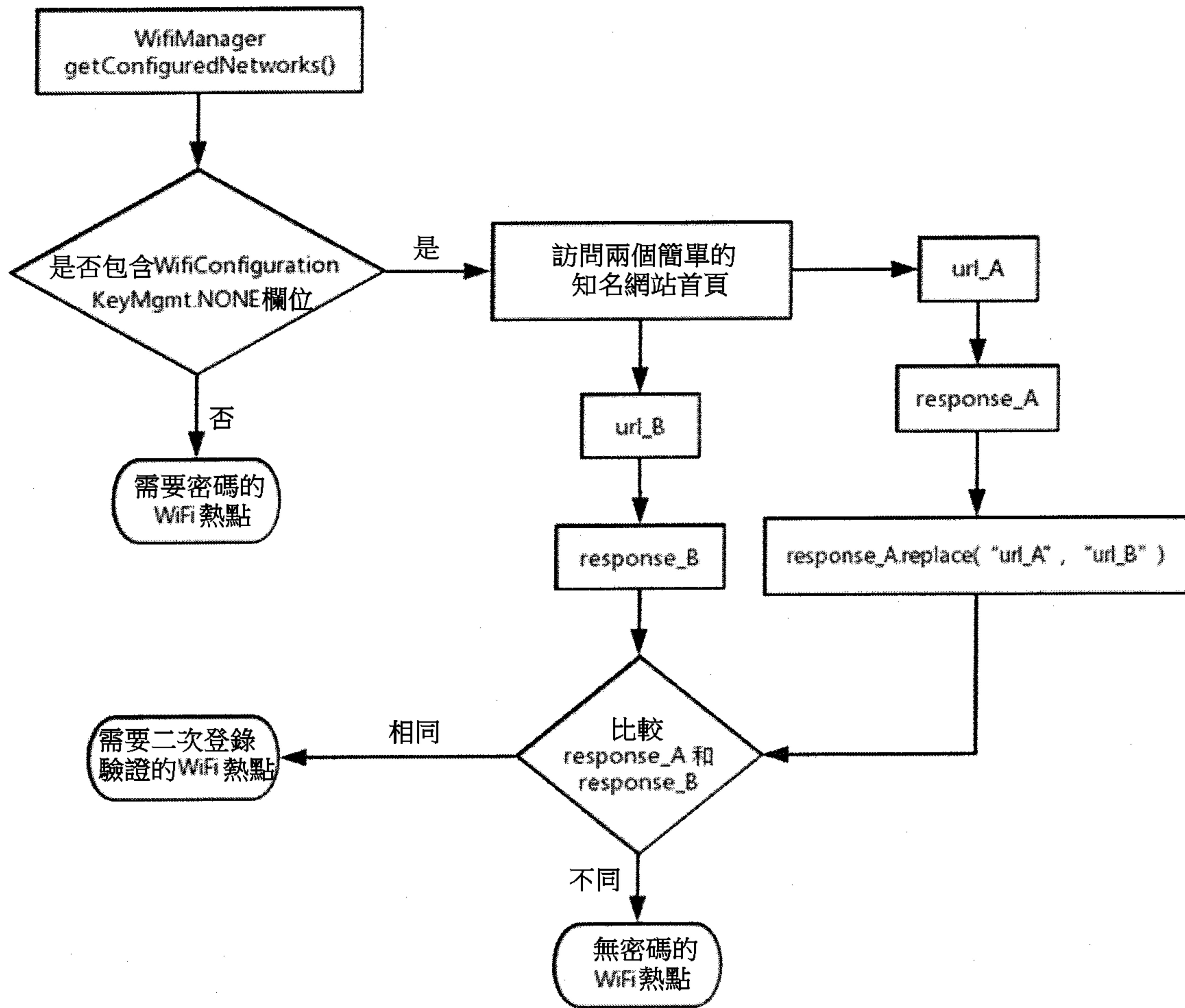


圖 2D

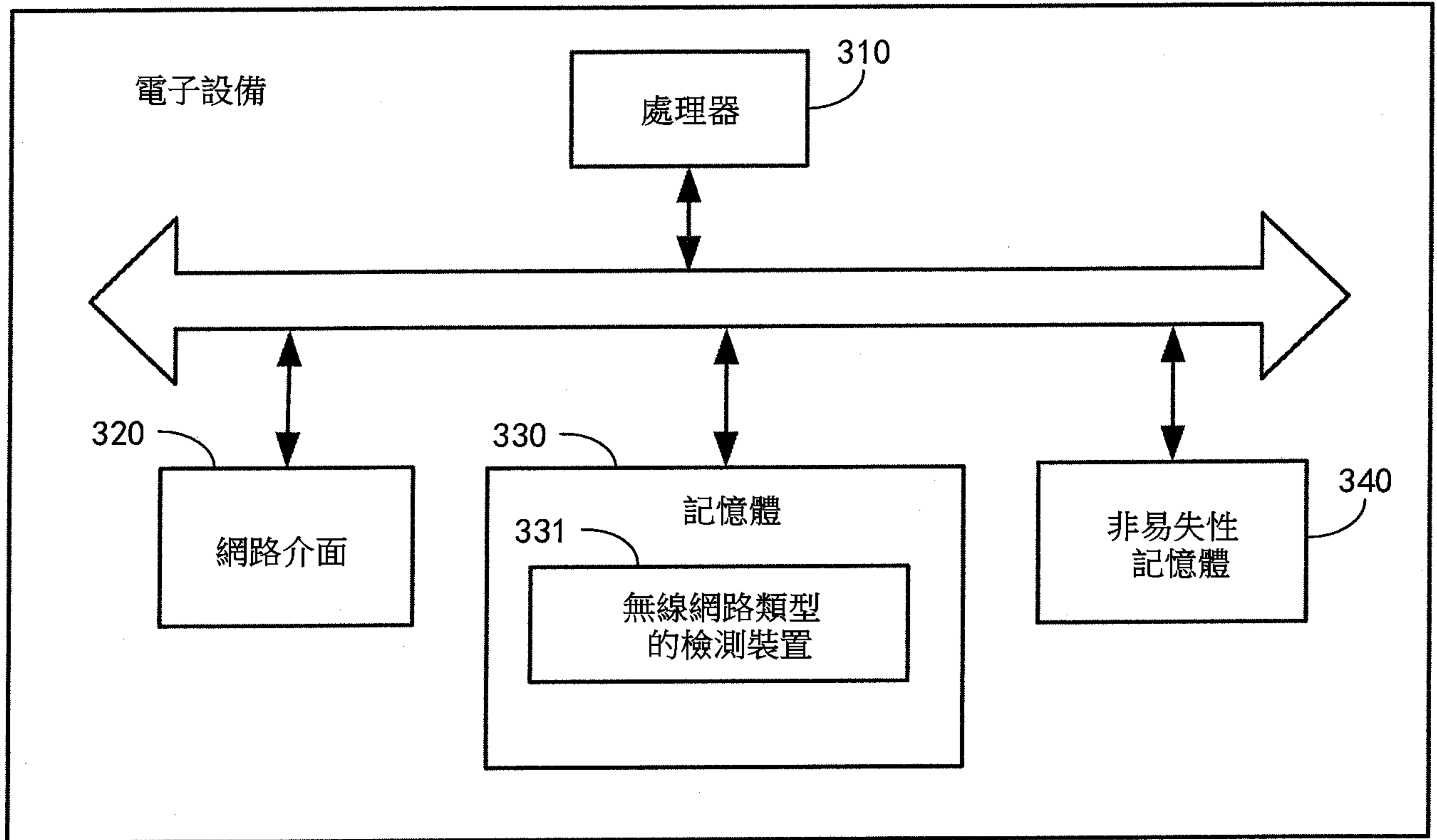


圖 3

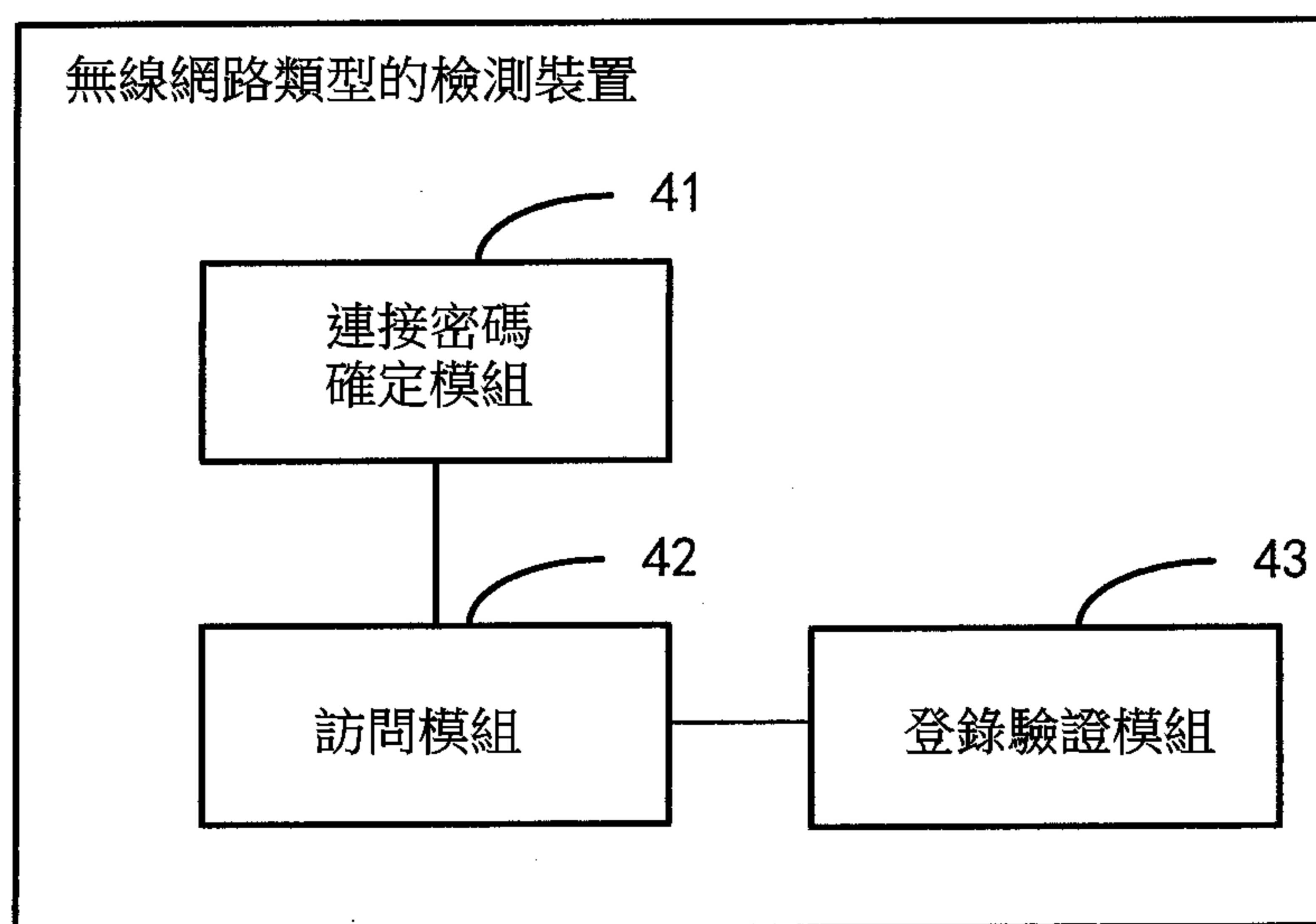


圖 4