



(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 I789350 B

(45)公告日：中華民國 112 (2023) 年 01 月 11 日

(21)申請案號：106115669

(22)申請日：中華民國 106 (2017) 年 05 月 11 日

(51)Int. Cl. : H04W12/08 (2021.01)

H04W12/00 (2021.01)

(30)優先權：2016/08/18 中國大陸

201610688098.3

(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：郭鎮龍 (CN)；趙磊 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 103368958A

US 2014/0344889A1

US 2015/0188949A1

WO 2015/188718A1

審查人員：王樂民

申請專利範圍項數：10 項 圖式數：8 共 37 頁

(54)名稱

W I F I 安全防護系統、無線網路防護方法、裝置及電子設備

(57)摘要

本申請提供一種 WIFI 安全防護系統、無線網路防護方法、裝置及電子設備，該方法包括：獲取所述電子設備接入的無線網路的類型；當所述無線網路的類型為設定類型時，對預設應用程式開始監控；確定所述預設應用程式啟動；控制所述電子設備透過虛擬私人網路 VPN 建立與第一伺服器的連接。在本申請的技術方案可以確保電子設備在接入到無線網路時的安全性並節省虛擬私人網路的網路流量。

指定代表圖：

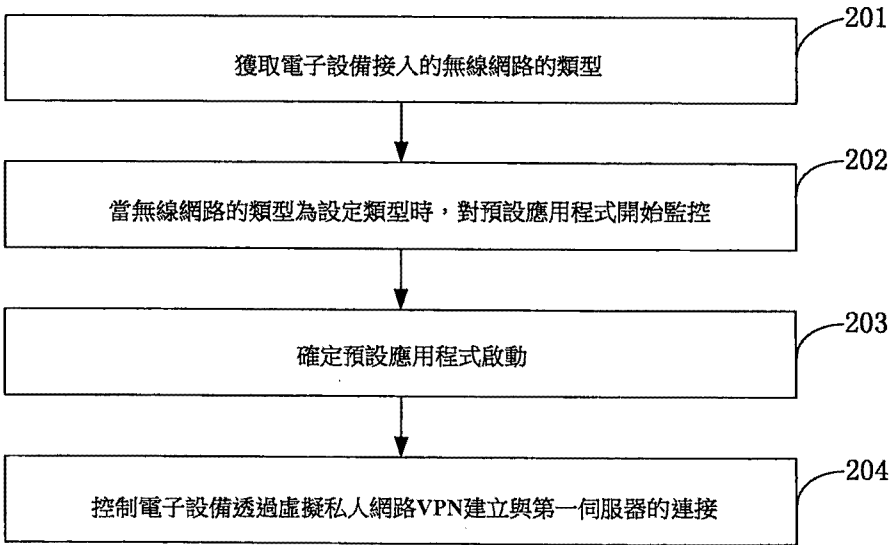


圖 2A

I789350

【發明摘要】

【中文發明名稱】

WIFI 安全防護系統、無線網路防護方法、裝置及電子設備

【中文】

本申請提供一種 WIFI 安全防護系統、無線網路防護方法、裝置及電子設備，該方法包括：獲取所述電子設備接入的無線網路的類型；當所述無線網路的類型為設定類型時，對預設應用程式開始監控；確定所述預設應用程式啟動；控制所述電子設備透過虛擬私人網路 VPN 建立與第一伺服器的連接。在本申請的技術方案可以確保電子設備在接入到無線網路時的安全性並節省虛擬私人網路的網路流量。

【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】

WIFI 安全防護系統、無線網路防護方法、裝置及電子設備

【技術領域】

本申請關於網路安全技術領域，尤其關於一種 WIFI 安全防護系統、無線網路連接安全防護方法、裝置及電子設備。

【先前技術】

當智能手機接入到商場、餐廳、影院、KTV、酒吧、機場、酒店、地鐵等公共場所的公共免費無線保真（Wireless-Fidelity，簡稱為 WIFI）網路時，由於大量互相不認識的用戶會共用該公共免費 WIFI 網路的 WIFI 密碼，如果合法用戶透過操作智慧手機接入到該公共免費 WIFI 網路，並且透過智慧手機進行了支付行為等敏感操作，該支付行為會被其他非法用戶惡意監測，合法用戶的支付密碼會被非法用戶竊取，現有技術還不能夠保障用戶透過公共免費 WIFI 接入無線局域網時的安全問題。

【發明內容】

本申請提供一種新的技術方案，可以確保電子設備在接入到無線網路時的安全性並節省虛擬私人網路（Virtual

Private Network，簡稱為 VPN）的網路流量。

為實現上述目的，本申請提供技術方案如下：

根據本申請的第一方面，提出了一種 WIFI 安全防護系統，包括：電子設備、第一伺服器、第二伺服器，所述電子設備上安裝有用戶端，所述第一伺服器與所述用戶端資料連接，所述第二伺服器為提供資金類應用程式的伺服器；其中，所述用戶端，用於在確定已連接的 WIFI 的類型為風險 WIF 並且資金類應用程式啟動時，控制所述電子設備透過虛擬私人網路建立與所述第一伺服器的連接；所述第一伺服器，用於透過所述虛擬私人網路接收由所述資金類應用程式觸發產生的消息，將所述消息轉發至所述第二伺服器，所述第二伺服器用於對所述消息進行處理。

根據本申請的第二方面，提出了一種無線網路連接安全防護方法，應用於電子設備，包括：獲取所述電子設備接入的無線網路的類型；當所述無線網路的類型為設定類型時，對預設應用程式開始監控；確定所述預設應用程式啟動；控制所述電子設備透過虛擬私人網路 VPN 建立與第一伺服器的連接。

根據本申請的協力廠商面，提出了一種無線網路連接安全防護裝置，應用於電子設備，包括：獲取單元，用於獲取所述電子設備接入的無線網路的類型；監控單元，用於當所述獲取單元獲取到的所述無線網路的類型為設定類型時，對預設應用程式開始監控；確定單元，用於確定所述預設應用程式啟動；控制單元，用於在所述確定單元確

定所述預設應用程式啟動時，控制所述電子設備透過 VPN 建立與第一伺服器的連接。

根據本申請的第四方面，提出了一種電子設備，包括：

處理器；用於儲存所述處理器可執行指令的記憶體；

其中，所述處理器，用於獲取所述電子設備接入的無線網路的類型；當所述無線網路的類型為設定類型時，對預設應用程式開始監控；確定所述預設應用程式啟動；控制所述電子設備透過虛擬私人網路 VPN 建立與第一伺服器的連接。

由以上技術方案可見，本申請可以對預設應用程式的任何操作進行監控，確保透過設定類型的無線網路傳輸與預設應用程式相關的資訊時的安全性。由於 VPN 的秘密頻道只有在預設應用程式啟動時才建立，因此可以避免電子設備由於長期連接 VPN 對第一伺服器造成的壓力過大的問題，節省了 VPN 的流量。

【圖式簡單說明】

圖 1 示出了根據本發明的一示例性實施例的 WIFI 安全防護系統的結構示意圖；

圖 2A 示出了根據本發明的一示例性實施例的無線網路連接安全防護方法的流程示意圖；

圖 2B 示出了圖 2A 所示實施例的無線網路連接安全防護方法的場景圖；

圖 3A 示出了根據本發明的另一示例性實施例的無線網路連接安全防護方法的流程示意圖；

圖 3B 示出了圖 3A 所示實施例的無線網路連接安全防護方法的場景圖；

圖 4A 示出了根據本發明的再一示例性實施例的無線網路連接 I 安全防護方法的流程示意圖；

圖 4B 示出了圖 4A 所示實施例的無線網路連接防護方法的場景圖之一；

圖 4C 示出了圖 4A 所示實施例的無線網路連接安全防護方法的場景圖之二；

圖 5A 示出了根據本發明的又一示例性實施例的無線網路連接安全防護方法的流程示意圖；

圖 5B 示出了圖 5A 所示實施例的無線網路連接安全防護方法的場景圖之一；

圖 5C 示出了圖 5A 所示實施例的無線網路連接安全防護方法的場景圖之二；

圖 6 示出了根據本發明的又一示例性實施例的無線網路連接安全防護方法的流程示意圖；

圖 7 示出了根據本發明的一示例性實施例的無線網路連接安全防護裝置的結構示意圖；

圖 8 示出了根據本發明的一示例性實施例的電子設備的結構示意圖。

【實施方式】

這裡將詳細地對示例性實施例進行說明，其示例表示在附圖中。下面的描述關於附圖時，除非另有表示，不同附圖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申請相一致的所有實施方式。相反，它們僅是與如所附申請專利範圍第書中所詳述的、本申請的一些方面相一致的裝置和方法的例子。

在本申請使用的術語是僅僅出於描述特定實施例的目的，而非旨在限制本申請。在本申請和所附申請專利範圍第書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，儘管在本申請可能採用術語第一、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，在不脫離本申請範圍的情況下，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”。

本申請關於到的基本概念：

用戶端：指與伺服器相對應，為用戶提供本機服務的程式。

應用程式：也稱為 APP，指安裝在智慧手機上的軟

體。

VPN：指在公用網絡上建立的私人網路，在該私人網路進行加密通訊。

圖 1 示出了根據本發明的一示例性實施例的 WIFI 安全防護系統的結構示意圖；如圖 1 所示，系統包括：電子設備 11、第一伺服器 12、第二伺服器 13，電子設備 11 上安裝有用戶端 111，第一伺服器 12 與用戶端 111 資料連接，第二伺服器 13 為提供資金類應用程式的伺服器。

其中，用戶端 111，用於在確定已連接的 WIFI 的類型為風險 WIFI 時，控制用戶端 111 進入 WIFI 防護的狀態，檢測資金類應用程式是否啟動，當資金類應用程式啟動時，控制電子設備 11 透過 VPN 建立與第一伺服器 12 的連接。

在一實施例中，風險 WIFI 可以為免費 WIFI、無密碼 WIFI、陌生 WIFI（電子設備 11 從未登錄過的 WIFI）。在一實施例中，資金類應用程式可以為支付類應用程式，例如，支付寶。

第一伺服器 12，用於透過 VPN 接收由資金類應用程式觸發產生的消息，將消息轉發至第二伺服器 13，第二伺服器 13 用於對消息進行處理。在一實施例中，由資金類應用程式觸發產生的消息可以為轉帳消息、支付消息、訂單消息等等。

在一實施例中，用戶端 111 還用於在 WIFI 防護的狀態，檢測當前介面是否顯示資金類應用程式，當當前介面

不顯示資金類應用程式時，斷開 VPN 並控制用戶端 111 透過該風險 WIFI 保持與第一伺服器 12 的連接。

本實施例提供的 WIFI 安全防護系統中，在確定已連接的 WIFI 的類型為風險 WIFI 時，用戶端 111 進入 WIFI 防護的狀態，當在 WIFI 防護的狀態下資金類應用程式啟動時，控制用戶端 111 透過 VPN 建立與第一伺服器 12 的連接，從而可以確保用戶端 111 對資金類應用程式的任何操作進行監控，並將資金類應用程式的任何操作產生的消息透過 VPN 發送給第一伺服器 12，避免非法用戶竊取合法用戶在資金類應用程式的支付密碼，確保電子設備 11 透過公共免費 WIFI 接入無線局域網時交易的安全性。由於 VPN 的秘密頻道只有在資金類應用程式啟動時才建立，避免用戶端 111 由於長期連接 VPN 對第一伺服器 12 造成的壓力過大的問題，節省了 VPN 的流量。

圖 2A 示出了根據本發明的一示例性實施例的無線網路連接安全防護方法的流程示意圖，圖 2B 示出了圖 2A 所示實施例的無線網路連接安全防護方法的場景圖；本實施例結合圖 1 進行示例性說明，本實施例可應用在圖 1 所示的電子設備 11 上，透過用戶端 111 實現，如圖 2A 所示，包括如下步驟：

步驟 201，獲取電子設備接入的無線網路的類型。

在一實施例中，以無線網路為 WIFI 網路為例進行示例性說明，則設定類型可以為免費 WIFI、無密碼 WIFI、陌生 WIFI 等，可以根據實際需求來確定設定類型，本申

請對設定類型的具體 WIFI 類型不做限制。

步驟 202，當無線網路的類型為設定類型時，對預設應用程式開始監控。

在一實施例中，預設應用程式可以為用戶端 111 需要保護的關於到用戶資金或者個人隱私的應用程式，例如，支付寶等支付類應用程式，本領域技術人員可以理解的是，本申請僅以支付類應用程式為例進行示例性說明，支付類應用程式並不能形成對預設應用程式的限制，當用戶需要對電子設備 11 上的任意應用程式需要安全防護時，均可以將任意應用程式視為本申請中的預設應用程式，執行本申請中的安全防護方法的流程。在一實施例中，監控的內容可以包括：預設應用程式是否啟動以及透過預設應用程式進行的操作。

步驟 203，確定預設應用程式啟動。

步驟 204，控制電子設備透過虛擬私人網路 VPN 建立與第一伺服器的連接。

在一實施例中，VPN 可以為電子設備 11 與第一伺服器 12 之間的私人網路，由預設應用程式觸發的消息均可以透過該私人網路傳輸給第一伺服器 12，第一伺服器 12 可以再將由預設應用程式觸發的消息轉發給第二伺服器 13。

在一示例性場景中，以用戶端 111 為阿裡錢盾並且第一伺服器 12 為提供阿裡錢盾的伺服器為例進行示例性說明，電子設備 11 透過商場提供的 WIFI 接入到無線局域

網，當用戶端 111 確定該 WIFI 的類型為免費 WIFI 時，用戶端 111 進入監控過程中，在監控過程中，用戶端 111 對預設應用程式開始監控。檢測是否有支付寶等資金類應用程式啟動，如圖 2B 所示，當確定支付寶啟動時，用戶端 111 控制電子設備在電量欄 112 處展示了阿裡錢盾的 WIFI 防護的狀態已經開啟，用戶端 111 控制電子設備 11 透過 VPN 建立與第一伺服器 12 的連接，從而可以由支付寶觸發生成的相關消息透過 VPN 加密傳輸至第一伺服器 12，第一伺服器 12 在將該相關消息進行解密後轉發給第二伺服器 13，第二伺服器 13 實現對支付寶進行相應的業務處理。

由上述描述可知，本發明實施例可以對預設應用程式的任何操作進行監控，確保透過設定類型的無線網路傳輸與預設應用程式相關的資訊時的安全性。由於 VPN 的秘密頻道只有在預設應用程式啟動時才建立，因此可以避免電子設備由於長期連接 VPN 對第一伺服器造成的壓力過大的問題，節省了 VPN 的流量。

圖 3A 示出了根據本發明的另一示例性實施例的無線網路連接安全防護方法的流程示意圖，圖 3B 示出了圖 3A 所示實施例的無線網路連接安全防護方法的場景圖；本實施例在上述實施例的基礎上，以在設定狀態下如何斷開 VPN 的連接為例並結合圖 1 和圖 2B 進行示例性說明，如圖 3A 所示，包括如下步驟：

步驟 301，在監控過程中，控制電子設備在當前介面

上的設定位置展示用戶端處於設定狀態的提示內容。

在一實施例中，如圖 2B 所示，當前介面的支付寶頂部的電量欄 112 中，顯示了阿裡錢盾處於防護狀態的提示內容，該提示內容可以透過動畫的方式展示在電量欄 112 中。

步驟 302，檢測當前介面是否顯示預設應用程式的介面，當當前介面不顯示預設應用程式的介面時，執行步驟 302，當當前介面顯示預設應用程式的介面時，繼續對預設應用程式進行監測。

在一實施例中，用戶端 11 可以透過與電子設備 11 的作業系統之間的交互確定當前介面是否顯示支付寶的用戶介面，如圖 3B，電子設備 11 的當前介面顯示為作業系統的主介面，表示支付寶應用程式已經在當前介面上不顯示。

步驟 303，當當前介面不顯示預設應用程式的介面時，控制電子設備斷開 VPN 並控制用戶端透過該已連接的 WIFI 保持與第一伺服器的連接。

在一實施例中，當支付寶已經不在當前介面顯示時，則表示用戶端 111 可以不用處於監控狀態，或者仍處於監控狀態的情形下不用對支付寶進行檢測，用戶端 111 可以斷開 VPN，透過已連接的 WIFI 繼續保持與第一伺服器的連接，從而可以確保用戶能夠透過該已連接的 WIFI 訪問其它安全級別較低的應用程式，例如，視頻應用程式等，以節省用戶的網路流量。

步驟 304，當電子設備斷開 VPN 時，控制電子設備取消提示內容在設定位置的展示。

如圖 3B，當用戶端 111 需要控制電子設備 11 斷開 VPN 時，當電子設備 11 斷開 VPN 時，電量欄 112 處於正常顯示狀態，不再顯示圖 2B 所示的提示內容。

本實施例中，透過檢測當前介面是否顯示預設應用程式，當當前介面不再顯示預設應用程式時，控制電子設備斷開 VPN，由此可以大大降低用戶端對第一伺服器透過 VPN 訪問的壓力；透過控制電子設備取消提示內容在設定位置的展示，可以方便用戶及時獲知用戶端的當前狀態。

圖 4A 示出了根據本發明的再一示例性實施例的無線網路連接安全防護方法的流程示意圖，圖 4B 示出了圖 4A 所示實施例的無線網路連接安全防護方法的場景圖之一，圖 4C 示出了圖 4A 所示實施例的無線網路連接安全防護方法的場景圖之二；本實施例在上述實施例的基礎上，以在監控狀態下如何控制用戶端的圖示的顯示為例並結合圖 1 進行示例性說明，如圖 4A 所示，包括如下步驟：

步驟 401，在監控過程中，檢測用戶端的介面是否從當前介面退出，當用戶端的介面從當前介面退出時，執行步驟 402，當用戶端的介面未從當前介面退出時，繼續處於監控過程中。

步驟 402，當用戶端的介面從當前介面退出時，在當前介面顯示用於提示預設應用程式處於被監控過程中對應的圖示。

在一示例性場景中，如圖 4B 所示，當用戶端 111 未處於監控過程中時，如果檢測到用戶端 111 的介面從當前介面退出，則可以在電子設備 11 的當前介面顯示用戶端 111 對應的圖示 110，該圖示 110 的形狀可以與用戶端 111 在用戶介面上的圖示相一致，例如，形狀可以相同或者相似。如圖 4C 所示，當用戶端 111 處於監控過程中時，如果檢測到用戶端 111 的介面從當前介面退出，則可以在電子設備 11 的當前介面顯示用於提示預設應用程式處於被監控過程中對應的圖示，例如，圖 4B 所示的圖示 113。在一實施例中，圖示 110 和圖示 113 可以為懸浮圖示，當檢測到用戶點擊並移動圖示 110 或者圖示 113 時，可以根據用戶手指的觸控位置將圖示 110 或者圖示 113 移動到當前介面上的任意位置。

本實施例中，透過在用戶介面上顯示與設定狀態對應的圖示，可以使用戶透過圖示 113 直觀獲知用戶端 111 目前所處的狀態。

圖 5A 示出了根據本發明的又一示例性實施例的無線網路連接安全防護方法的流程示意圖，圖 5B 示出了圖 5A 所示實施例的無線網路連接安全防護方法的場景圖之一，圖 5C 示出了圖 5A 所示實施例的無線網路連接安全防護方法的場景圖之二；本實施例在上述實施例的基礎上，以在斷開已連接的 WIFI 的情形下如何提示設定狀態結束並顯示關於預設應用程式已保護的操作內容為例並結合圖 1 進行示例性說明，如圖 5A 所示，包括如下步驟：

步驟 501，確定電子設備是否斷開已連接的 WIFI，當電子設備斷開已連接的 WIFI 時，執行步驟 502，當已連接的 WIFI 保持連接狀態時，繼續執行上述圖 2A 所示實施例的方法流程。

在一實施例中，用戶端 111 可以與電子設備 11 的交互來得到 WIFI 是否已經斷開。

步驟 502，當電子設備斷開已連接的 WIFI 時，確定用戶端是否為首次進入設定狀態，當用戶端為首次進入設定狀態時執行步驟 503，當用戶端為非首次進入設定狀態時，執行步驟 504。

步驟 503，當用戶端為首次進入設定狀態時，透過第一懸浮層或者第一彈出消息的方式提示監控過程結束，流程結束。

在步驟 502 和步驟 503 中，若用戶端 111 首次進入設定狀態，如圖 5B 所示，如果電子設備 11 需要離開該已連接的 WIFI，則可以在電子設備 11 的顯示幕上顯示第一懸浮層或者第一彈出消息，透過第一懸浮層或者第一彈出消息提示用戶該設定狀態結束。在一實施例中，若電子設備 11 的作業系統給用戶端 111 開設有懸浮窗的許可權，則彈出第一懸浮層，若電子設備 11 的作業系統未給用戶端 111 開設懸浮窗的許可權，則彈出第一彈出消息。

步驟 504，當用戶端為非首次監控應用程式時，確定是否對預設應用程式上的預設操作進行過保護，當對預設應用程式上的預設操作進行過保護時，執行步驟 505。

步驟 505，當對預設應用程式上的預設操作進行過保護時，透過第二懸浮層或者第二彈出消息提示對預設應用程式上的預設操作進行過保護。

步驟 506，顯示截止到當前時間點進行保護的操作內容，流程結束。

在步驟 504-步驟 506 中，若用戶端 111 非首次進入設定狀態，如圖 5C 所示，用戶端 111 第二次進入設定狀態，如果電子設備 11 需要離開該已連接的 WIFI，則可以確定是否對支付寶上的轉帳操作進行了保護，如果對支付寶上的轉帳操作進行了保護，則可則彈出第二懸浮層或者第二彈出消息，例如，阿裡錢盾保護了支付寶的 5 次轉帳操作，攔截了 3 次釣魚網站。在一實施例中，若電子設備 11 的作業系統給用戶端 111 開設有懸浮窗的許可權，則彈出第二懸浮層，若電子設備 11 的作業系統未給用戶端 111 開設懸浮窗的許可權，則彈出第二彈出消息。

本實施例中，當斷開已連接的 WIFI 時，根據用戶端是首次進入設定狀態還是非首次進入設定狀態的不同，顯示不同的通知消息，可以方便用戶獲知用戶端對預設應用程式的保護情況，方便用戶瞭解用戶端對預設應用程式防護的結果。

圖 6 示出了根據本發明的又一示例性實施例的無線網路連接安全防護方法的流程示意圖；本實施例在上述實施例的基礎上，以在設定狀態下用戶端如何攔截釣魚網站為例並結合圖 1 進行示例性說明，如圖 6 所示，包括如下步

驟：

步驟 601，在監控過程中，確定訪問的統一資源定位符。

在一實施例中，用戶端 111 可以透過從電子設備 11 啟動的流覽器獲取到用戶需要訪問的統一資源定位符（Uniform Resource Locator，簡稱為 URL）。

步驟 602，將訪問的統一資源定位符與預設清單中儲存的統一資源定位符進行比較，預設清單用於記錄釣魚類統一資源定位符。

步驟 603，當訪問的統一資源定位符在預設清單中有記錄時，將訪問的統一資源定位符攔截。

在一實施例中，可以從第一伺服器 12 獲取預設列表，第一伺服器 12 可以搜集釣魚網站的 URL，並定期或者即時地更新到預設列表中，將預設清單發送至電子設備 11，以供用戶端 111 能夠採用最新的預設列表對釣魚網站進行攔截。

在另一實施例中，如圖 1 所示，用戶端 111 可以透過上述步驟 601 確定訪問的 URL，將 URL 發送給第一伺服器 12，第一伺服器 12 透過查找預設列表，以確定該 URL 是否被記錄在預設清單中，若該 URL 被記錄在預設清單中，第一伺服器 12 可以生成比較結果並將比較結果返回給電子設備 11，當用戶端 111 確定比較結果表示訪問的 URL 在預設清單中有記錄時，將訪問的 URL 攔截。

本實施例中，透過在監控過程中對釣魚網站進行攔

截，可以連接 WIFI 防護過程，訪問釣魚類 URL 時自動攔截，避免電子設備的用戶被釣魚網站欺騙。

圖 7 為根據本發明的一示例性實施例的無線網路連接安全防護裝置的結構示意圖；如圖 7 所示，該無線網路連接安全防護裝置可以包括：獲取單元 71、監控單元 72、確定單元 73、控制單元 74。其中：

獲取單元 71，用於獲取電子設備接入的無線網路的類型；

監控單元 72，用於當獲取單元 71 獲取到的無線網路的類型為設定類型時，對預設應用程式開始監控；

確定單元 73，用於確定預設應用程式啟動；

控制單元 74，用於控制電子設備透過 VPN 建立與第一伺服器的連接。

可選的，監控單元 72，還用於檢測當前介面是否顯示預設應用程式的介面；當當前介面不顯示預設應用程式的介面時，控制電子設備斷開虛擬私人網路並透過無線網路保持與第一伺服器的連接。

可選的，控制單元 74，還用於檢測當前介面是否顯示預設應用程式的介面；當當前介面不顯示預設應用程式的介面時，控制電子設備斷開虛擬私人網路並透過無線網路保持與第一伺服器的連接。

可選的，監控單元 72，還用於在監控過程中，檢測用戶端的介面是否從當前介面退出；當用戶端的介面從當前介面退出時，在當前介面顯示用於提示預設應用程式處

於被監控過程中的圖示。

可選的，確定單元 73，還用於確定電子設備是否斷開無線網路；當電子設備斷開無線網路時，確定是否為首次監控預設應用程式；當為首次監控預設應用程式時，透過第一懸浮層或者第一彈出消息的方式提示監控過程結束。

可選的，確定單元 73，還用於當為非首次進入監控預設應用程式時，確定是否對預設應用程式上的預設操作進行過保護；當對預設應用程式上的預設操作進行過保護時，透過第二懸浮層或者第二彈出消息提示對預設應用程式上的預設操作進行過保護；顯示截止到當前時間點進行保護的操作內容。

可選的，確定單元 73，還用於在監控過程中，確定訪問的統一資源定位符；將訪問的統一資源定位符與預設清單中儲存的統一資源定位符進行比較，預設清單用於記錄釣魚類統一資源定位符；當訪問的統一資源定位符在預設清單中有記錄時，將訪問的統一資源定位符攔截。

可選的，確定單元 73，還用於在監控過程中，確定訪問的統一資源定位符；將訪問的統一資源定位符發送至第一伺服器，第一伺服器將訪問的統一資源定位符與預設清單中儲存的統一資源定位符進行比較並返回比較結果，預設清單用於記錄釣魚類統一資源定位符；當比較結果表示訪問的統一資源定位符在預設清單中有記錄時，將訪問的統一資源定位符攔截。

對應於上述任一實施例提供的無線網路連接安全防護方法，本申請還提出了圖 8 所示的根據本發明的一示例性實施例的電子設備的示意結構圖。請參考圖 8，在硬體層面，該電子設備可包括處理器、內部匯流排、網路介面、記憶體以及非易失性記憶體，當然還可能包括其他業務所需要的硬體。處理器從非易失性記憶體中讀取對應的電腦程式到記憶體中然後運行，在邏輯層面上實現上述無線網路連接安全防護裝置。當然，除了軟體實現方式之外，本申請並不排除其他實現方式，比如邏輯器件抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯器件。

其中，處理器，用於獲取電子設備接入的無線網路的類型；當無線網路的類型為設定類型時，對預設應用程式開始監控；確定預設應用程式啟動；控制電子設備透過虛擬私人網路 VPN 建立與第一伺服器的連接。

本領域技術人員在考慮說明書及實踐這裡公開的發明後，將容易想到本申請的其它實施方案。本申請旨在涵蓋本申請的任何變型、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申請的一般性原理並包括本申請未公開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，本申請的真正範圍和精神由下面的申請專利範圍指出。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系

列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

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

【符號說明】

11：電子設備

12：第一伺服器

13：第二伺服器

71：獲取單元

72：監控單元

73：確定單元

74：控制單元

110：圖示

111：用戶端

112：電量欄

113：圖示

201、202、203、204：方法步驟

301、302、303、304：方法步驟

401、402：方法步驟

501、502、503、504、505、506：方法步驟

601、602、603：方法步驟

【發明申請專利範圍】

【第1項】

一種無線網路連接安全防護方法，應用於電子設備，其特徵在於，該方法包括：

由該電子設備上的用戶端獲取該電子設備接入的無線網路的類型；

由該用戶端至少根據該電子設備接入該無線網路的頻率，確定該無線網路的類型為風險WIFI；

確定該無線網路的類型為風險WIFI時，由該用戶端開啟WIFI防護的狀態，該用戶端在該電子設備接入該風險WIFI時進入該WIFI防護的狀態中操作；及

當在該WIFI防護的狀態下，進行以下步驟：

對預設應用程式開始監控，其中，該預設應用程式安裝在該電子設備上，該用戶端透過與該電子設備的作業系統之間的交互確定當前介面是否顯示該預設應用程式的用戶介面；

確定在該電子設備接入該風險WIFI時啟動該預設應用程式；

確定在該電子設備接入該風險WIFI時啟動該預設應用程式時，控制該電子設備透過虛擬私人網路VPN建立與第一伺服器的連接；

在該電子設備接入該風險WIFI時確定該預設應用程式不再處於活動狀態，其中，該預設應用程式不再處於活動狀態包括當當前介面不顯示該預設應用

程式時，表示該用戶端不用處於監控狀態，或者仍處於監控狀態的情形下不用對該預設應用程式進行檢測；及

當該應用程式不再使用時，斷開該電子設備與該第一伺服器之間的該虛擬私人網路VPN。

【第2項】

根據申請專利範圍第1項所述的方法，其中，該方法還包括：

在監控過程中，檢測當前介面是否顯示該預設應用程式的介面；及

該預設應用程式時不再處於活動狀態包括當該當前介面不顯示該預設應用程式的介面時。

【第3項】

根據申請專利範圍第2項所述的方法，其中，該方法還包括：

在監控過程中，控制該電子設備在該當前介面上的設定位置展示該用戶端處於監控過程中的提示內容；及

當斷開該虛擬私人網路時，控制該電子設備取消該提示內容在該設定位置的展示。

【第4項】

根據申請專利範圍第1項所述的方法，其中，該方法還包括：

在監控過程中，檢測用戶端的介面是否從當前介面退出；及

當該用戶端的介面從該當前介面退出時，在該當前介面顯示用於提示該預設應用程式處於被監控過程中的圖示。

【第5項】

根據申請專利範圍第1項所述的方法，其中，該方法還包括：

確定該電子設備是否斷開該無線網路；

當該電子設備斷開該無線網路時，確定是否為首次監控該預設應用程式；及

當為首次監控該預設應用程式時，透過第一懸浮層或者第一彈出消息的方式提示監控過程結束。

【第6項】

根據申請專利範圍第5項所述的方法，其中，該方法還包括：

當為非首次進入監控該預設應用程式時，確定是否對該預設應用程式上的預設操作進行過保護；

當對該預設應用程式上的預設操作進行過保護時，透過第二懸浮層或者第二彈出消息提示對該預設應用程式上的預設操作進行過保護；及

顯示截止到當前時間點進行保護的操作內容。

【第7項】

根據申請專利範圍第1項所述的方法，其中，該方法還包括：

在監控過程中，確定訪問的統一資源定位符；

將該訪問的統一資源定位符與預設清單中儲存的統一資源定位符進行比較，該預設清單用於記錄釣魚類統一資源定位符；及

當該訪問的統一資源定位符在該預設清單中有記錄時，將該訪問的統一資源定位符攔截。

【第8項】

根據申請專利範圍第1項所述的方法，其中，該方法還包括：

在監控過程中，確定訪問的統一資源定位符；

將該訪問的統一資源定位符發送至該第一伺服器，該第一伺服器將該訪問的統一資源定位符與預設清單中儲存的統一資源定位符進行比較並返回比較結果，該預設清單用於記錄釣魚類統一資源定位符；及

當該比較結果表示該訪問的統一資源定位符在該預設清單中有記錄時，將該訪問的統一資源定位符攔截。

【第9項】

一種無線網路連接安全防護裝置，應用於電子設備，其特徵在於，該裝置包括：

獲取單元，用於供該電子設備上的用戶端獲取該電子設備接入的無線網路的類型；

監控單元，用於供該用戶端至少根據該電子設備接入該無線網路的頻率，確定該獲取單元獲取到的該無線網路的類型為風險WIFI，其中，

該用戶端在確定該無線網路的類型為風險WIFI

時，開啟WIFI防護的狀態，該用戶端在該電子設備接入該風險WIFI時進入該WIFI防護的狀態中操作，且

該監控單元還用於當在該WIFI防護的狀態下對預設應用程式開始監控，其中，該預設應用程式安裝在該電子設備上，該用戶端透過與該電子設備的作業系統之間的交互確定當前介面是否顯示該預設應用程式的用戶介面；

確定單元，用於確定在該電子設備接入該風險WIFI時啟動該預設應用程式；及

控制單元，用於確定在該電子設備接入該風險WIFI時啟動該預設應用程式時，控制該電子設備透過VPN建立與第一伺服器的連接，其中，

該確定單元還用於在該電子設備接入該風險WIFI時確定該預設應用程式不再處於活動狀態，其中，該預設應用程式不再處於活動狀態包括當當前介面不顯示該預設應用程式時，表示該用戶端不用處於監控狀態，或者仍處於監控狀態的情形下不用對該預設應用程式進行檢測，且

該控制單元還用於當該應用程式不再使用時，斷開該電子設備與該第一伺服器之間的該虛擬私人網路VPN。

【第10項】

一種電子設備，其特徵在於，該電子設備包括：
處理器；及

用於儲存該處理器可執行指令的記憶體，其中，該處理器，用於

由該電子設備上的用戶端獲取該電子設備接入的無線網路的類型；

由該用戶端至少根據該電子設備接入該無線網路的頻率，確定該無線網路的類型為風險WIFI；

確定該無線網路的類型為風險WIFI時，由該用戶端開啟WIFI防護的狀態，該用戶端在該電子設備接入該風險WIFI時進入該WIFI防護的狀態中操作；及

當在該WIFI防護的狀態下，進行以下步驟：

對預設應用程式開始監控，其中，該預設應用程式安裝在該電子設備上，該用戶端透過與該電子設備的作業系統之間的交互確定當前介面是否顯示該預設應用程式的用戶介面；

確定在該電子設備接入該風險WIFI時啟動該預設應用程式；

確定在該電子設備接入該風險WIFI時啟動該預設應用程式時，控制該電子設備透過虛擬私人網路VPN建立與第一伺服器的連接；

在該電子設備接入該風險WIFI時確定該預設應用程式不再處於活動狀態，其中，該預設應用程式不再處於活動狀態包括當當前介面不顯示該預設應用程式時，表示該用戶端不用處於監控狀態，或者仍處於監控狀態的情形下不用對該

預設應用程式進行檢測；及

當該應用程式不再使用時，斷開該電子設備
與該第一伺服器之間的該虛擬私人網路VPN。

【發明圖式】

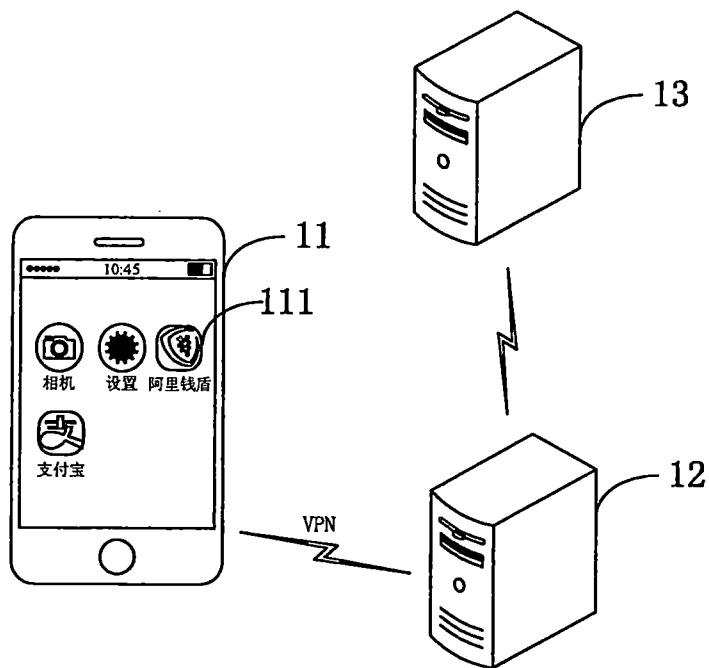


圖 1

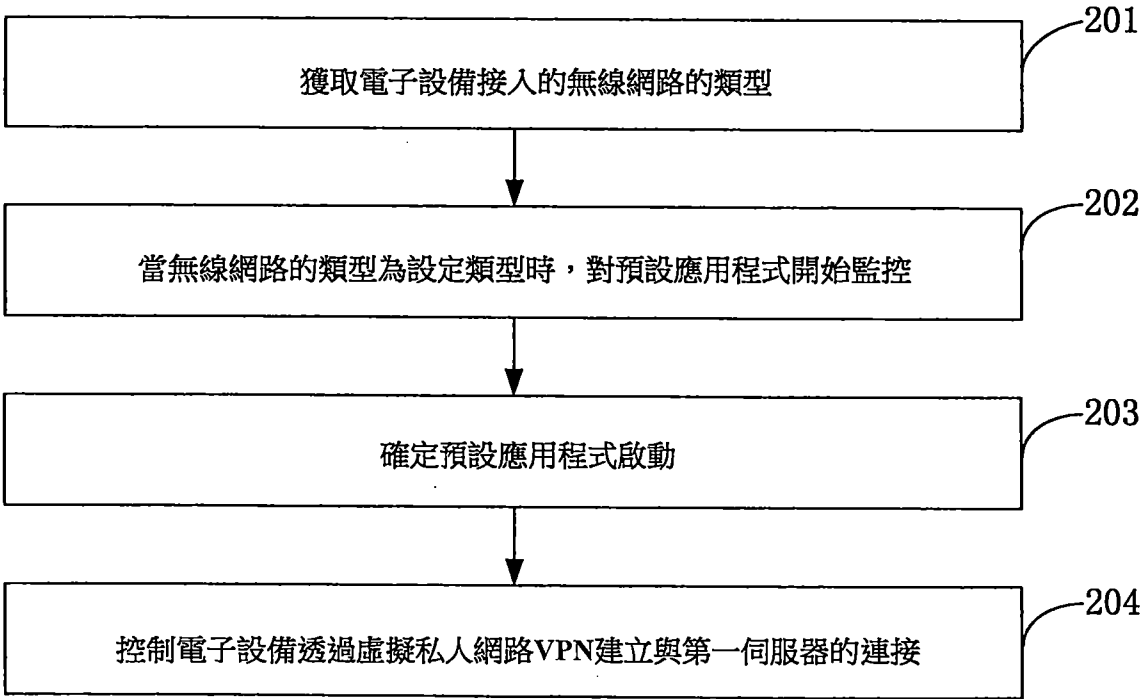


圖 2A

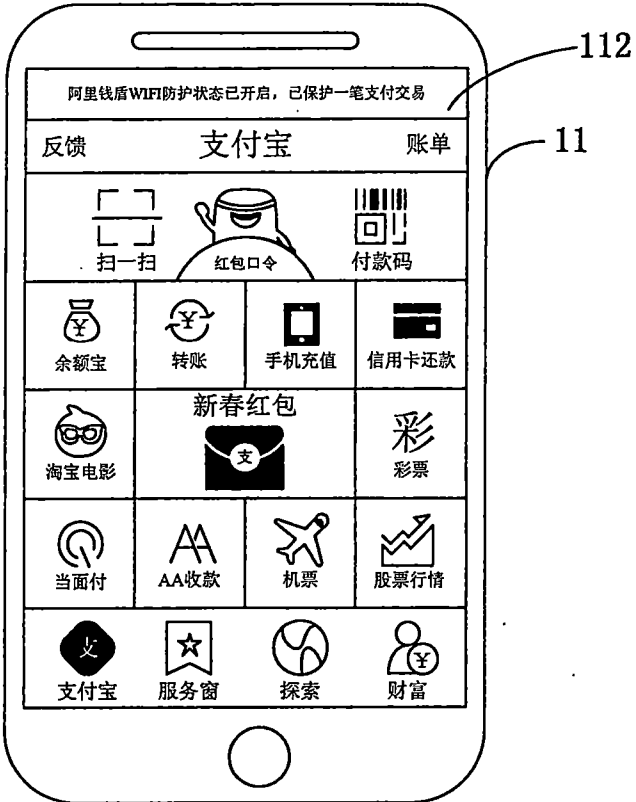


圖 2B

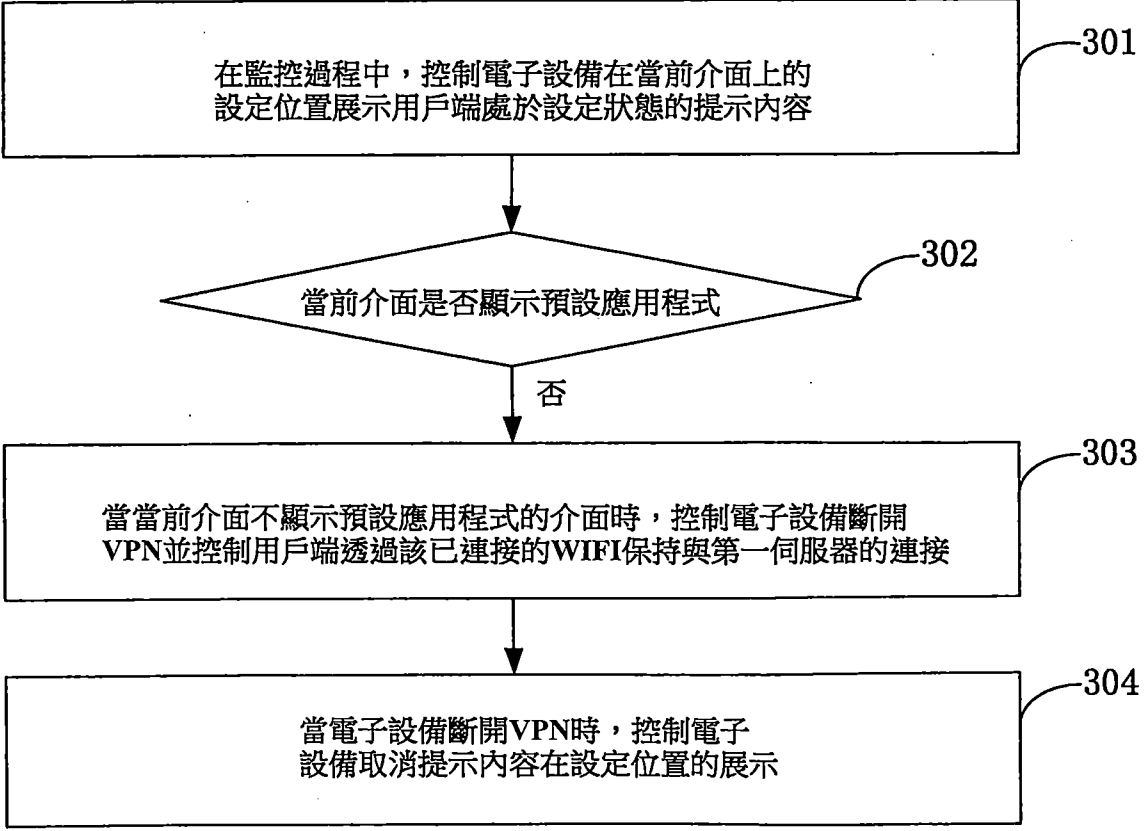


圖 3A

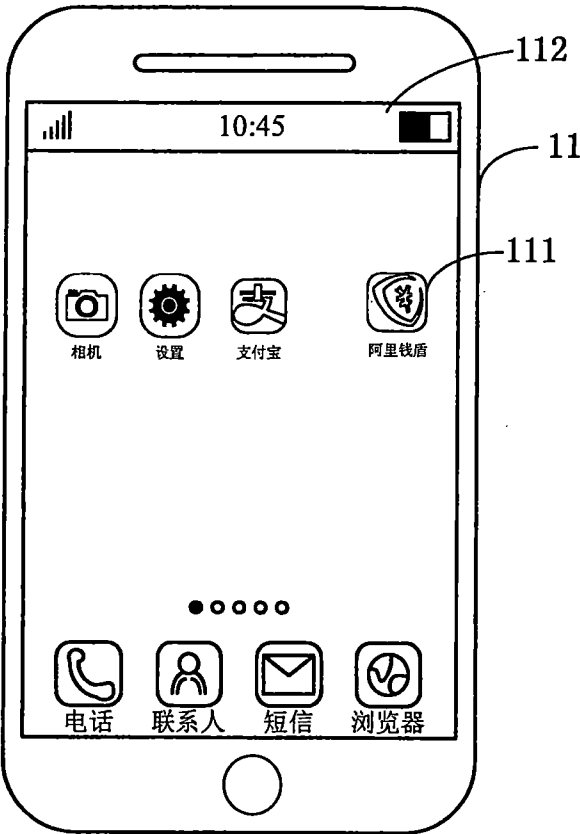


圖 3B

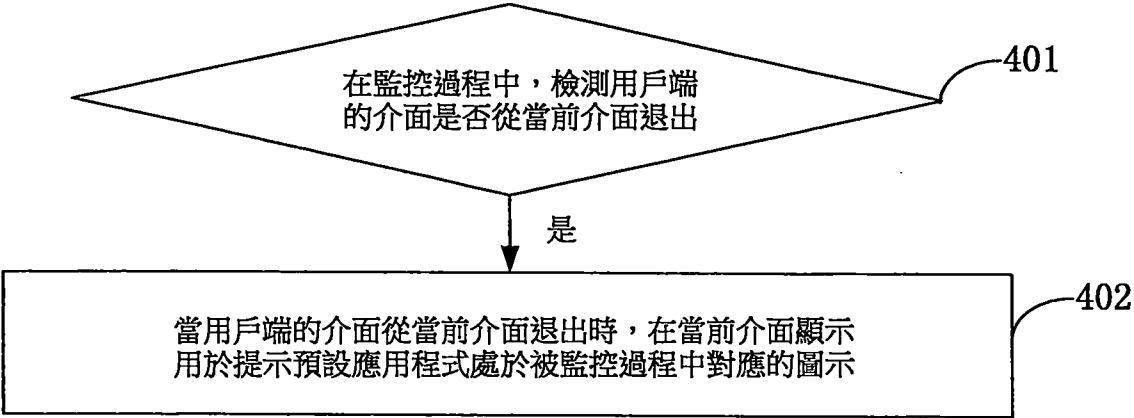


圖 4A

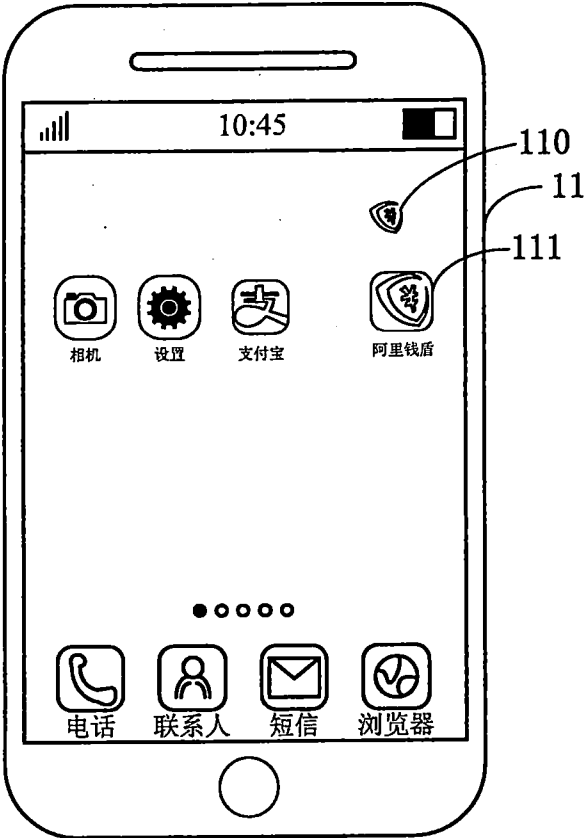


圖 4B

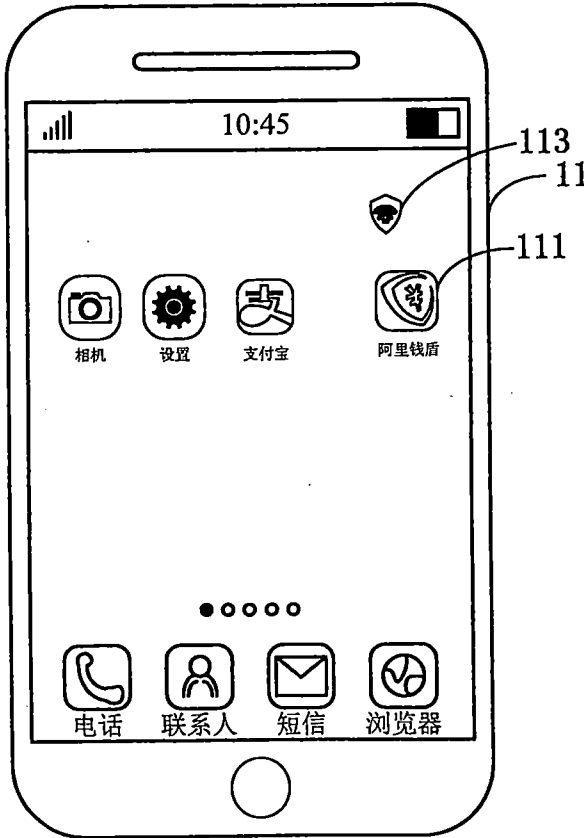


圖 4C

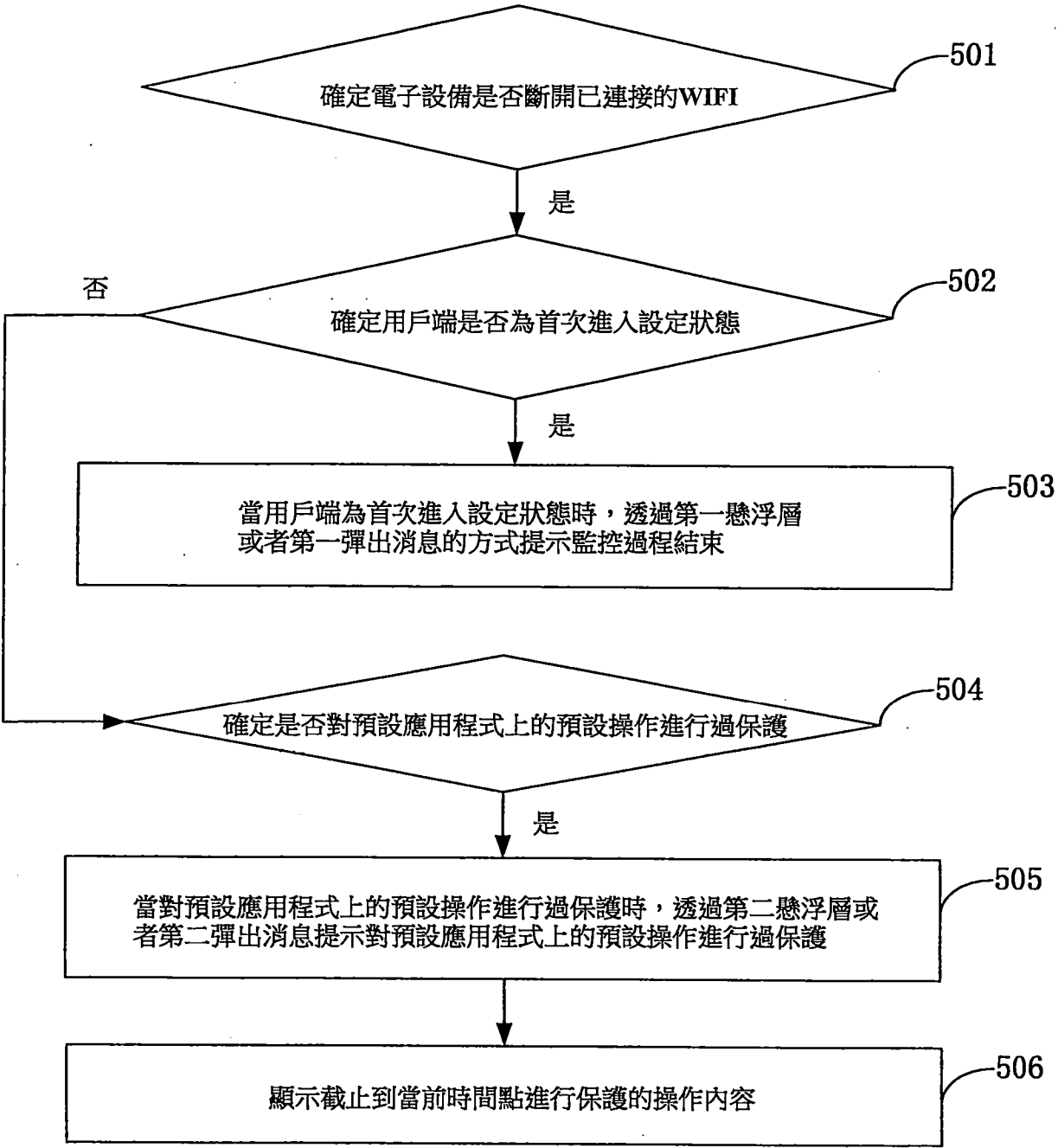


圖 5A

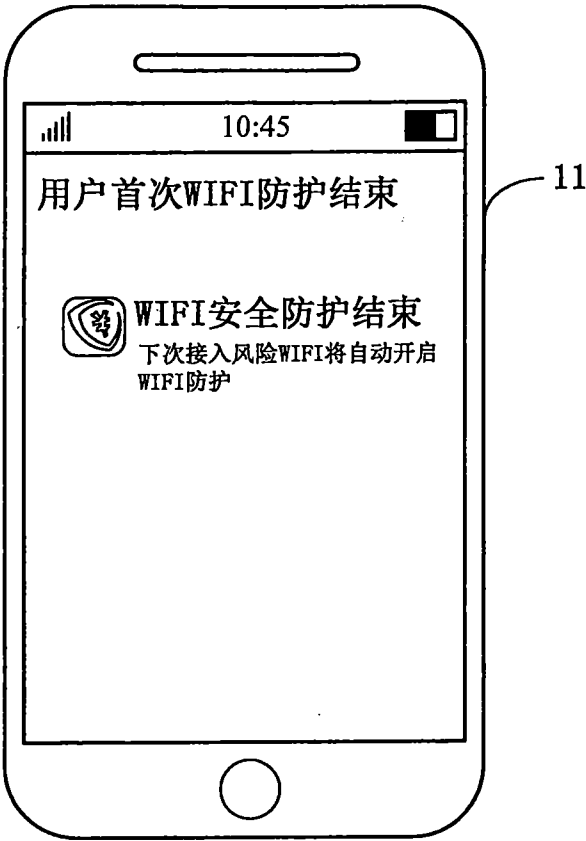


圖 5B

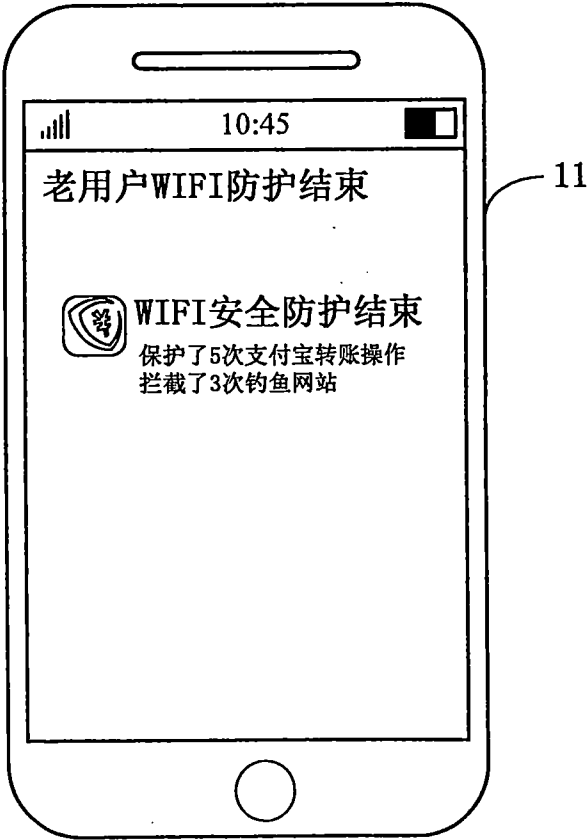


圖 5C

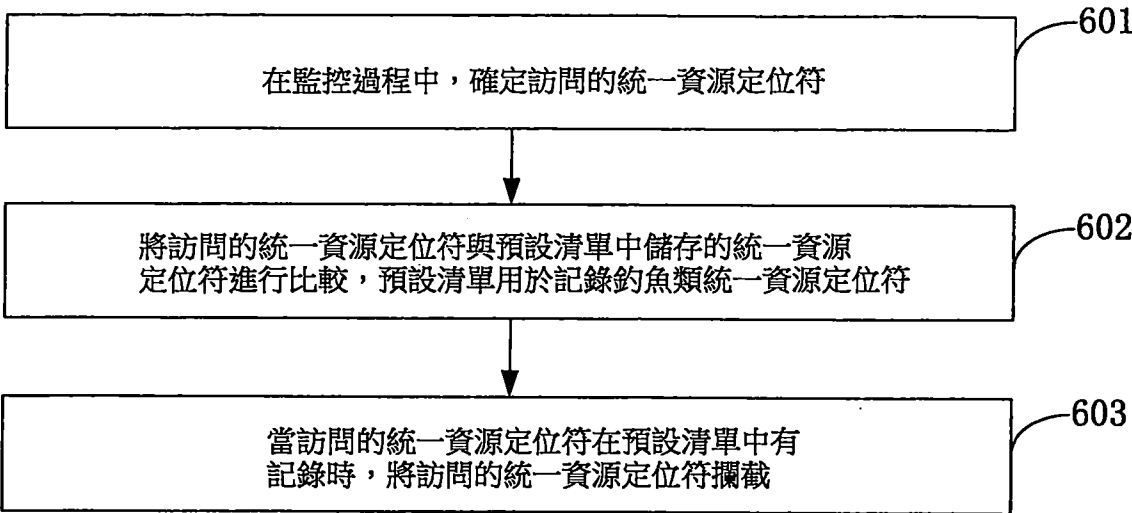


圖 6

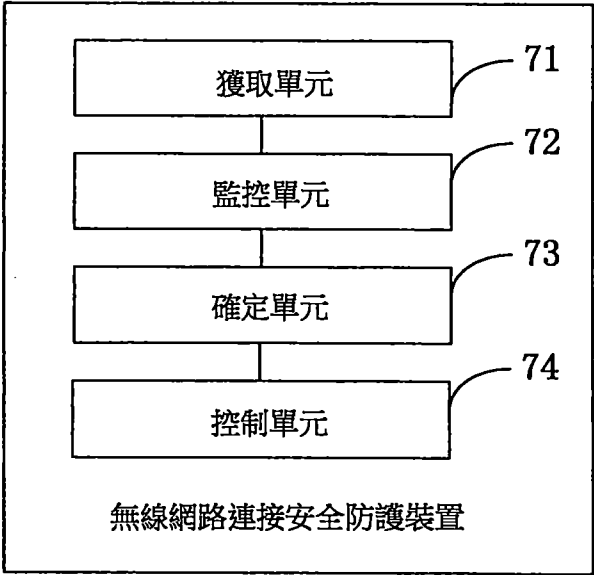


圖 7

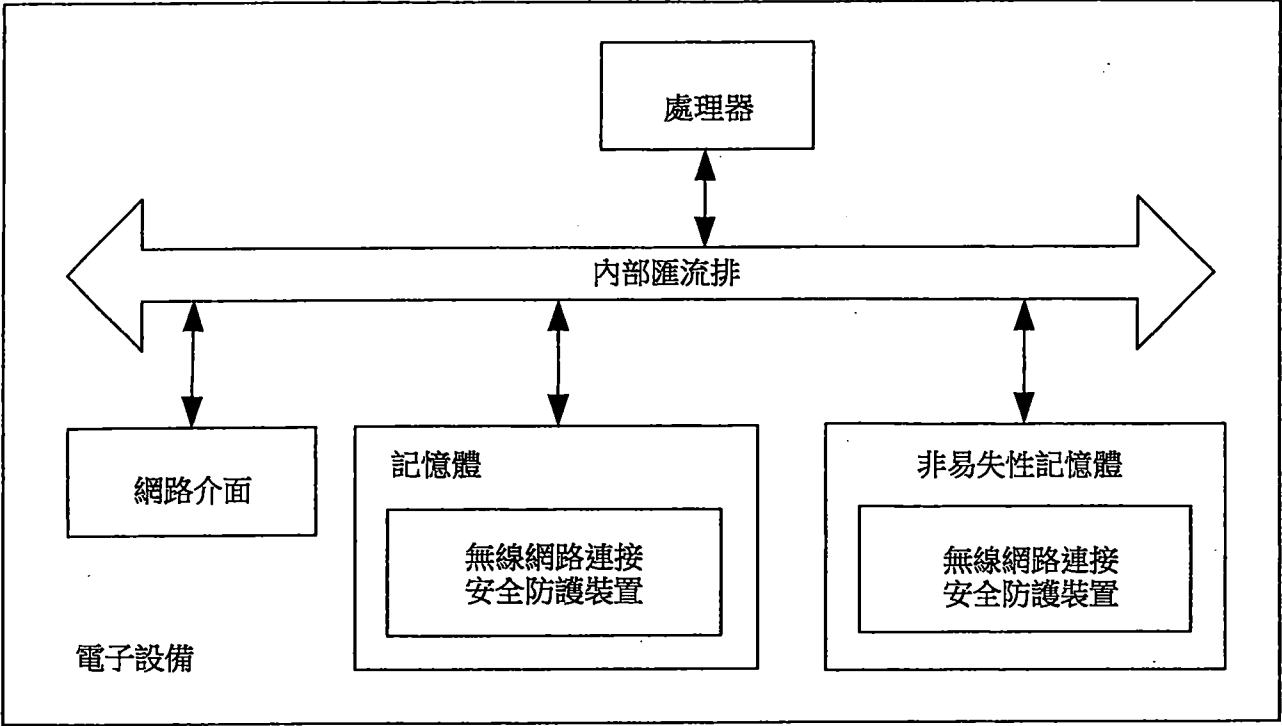


圖 8