



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0030671

(51)⁷

H04W 12/06; H04W 88/02; H04W 84/12

(13) **B**

(21) 1-2019-02807

(22) 28/06/2018

(86) PCT/US2018/040101 28/06/2018

(87) WO 2019/006175 03/01/2019

(30) 201710506456.9 28/06/2017 CN

(45) 25/01/2022 406

(43) 27/04/2020 385ASC

(73) Advanced New Technologies Co., Ltd. (KY)

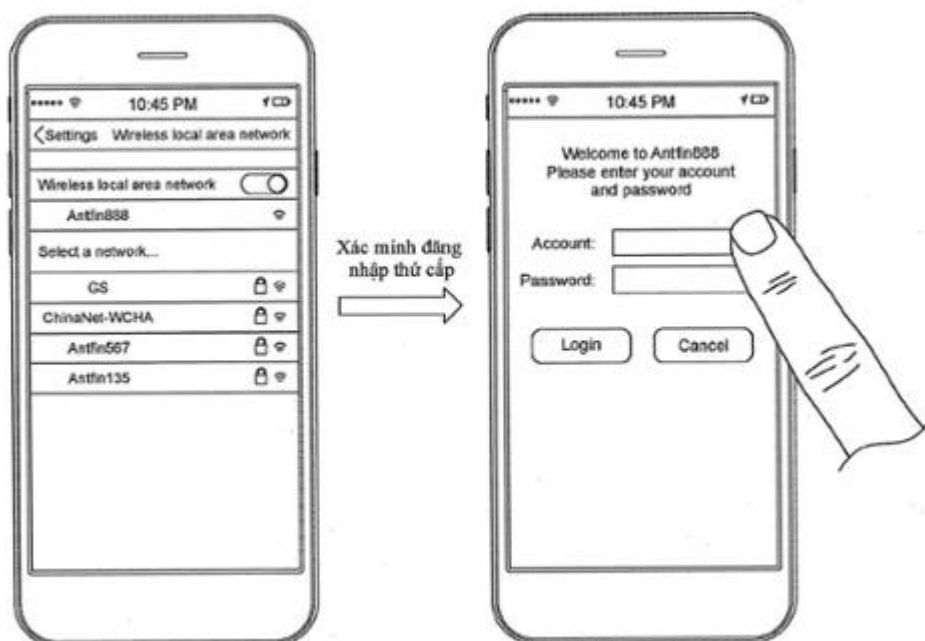
Cayman Corporate Centre, 27 Hospital Road, George Town, Grand Cayman KY1-9008, Cayman Islands

(72) WANG, Baochu (CN).

(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP PHÁT HIỆN KIỂU MẠNG KHÔNG DÂY VÀ THIẾT BỊ ĐIỆN TỬ

(57) Sáng chế đề cập đến phương pháp và thiết bị xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để truy cập Internet qua mạng không dây hay không dựa vào ít nhất một địa chỉ mạng chỉ định. Để đáp lại việc xác định rằng không cần mật khẩu, địa chỉ mạng chỉ định được truy cập. Việc liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không được xác định bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông và cụ thể là đề cập đến phương pháp và thiết bị phát hiện kiểu mạng không dây và thiết bị điện tử.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển của Internet di động, việc truy cập mạng không dây qua Wi-Fi ngày càng trở nên thường xuyên hơn đối với các thiết bị điện tử. Nhưng đồng thời, các vấn đề bảo mật Wi-Fi ngày càng trở nên đáng chú ý. Các thiết bị điện tử có thể kết nối với các trạm phát Wi-Fi không bảo mật, làm rò rỉ thông tin cá nhân, rò rỉ mật khẩu hoặc tài khoản bị đánh cắp.

Để tạo thuận lợi cho các kết nối người dùng và cho phép nhiều người dùng hơn truy cập vào các trạm phát (hotspot) Wi-Fi không bảo mật, hầu hết các trạm phát Wi-Fi không bảo mật không đặt mật khẩu đăng nhập. Do đó, hiện tại, nhiều ứng dụng công cụ bảo mật sẽ kiểm tra, sau khi thiết bị điện tử kết nối Wi-Fi, xem liệu Wi-Fi hiện tại có cần mật khẩu để kết nối hay không. Nếu không cần mật khẩu để kết nối, các ứng dụng bảo mật sẽ chặn thiết bị điện tử truy cập vào trạm phát Wi-Fi hoặc hiển thị thông báo bảo mật. Tuy nhiên, thỉnh thoảng sau khi kết nối với trạm phát Wi-Fi không có mật khẩu, người dùng vẫn được yêu cầu xác minh đăng nhập thứ cấp. Việc xác minh đăng nhập thứ cấp có nghĩa là mặc dù thiết bị không cần mật khẩu để kết nối với trạm phát Wi-Fi, màn hình đăng nhập sẽ hiện lên thiết bị khi truy cập Internet, yêu cầu người dùng nhập tên người dùng và mật khẩu để truy cập Internet.

Bản chất kỹ thuật của sáng chế

Trên cơ sở nêu trên, sáng chế đề xuất phương pháp và thiết bị phát hiện kiểu mạng không dây và thiết bị điện tử.

Phương pháp phát hiện kiểu mạng không dây bao gồm các bước: xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không; sau khi xác định rằng không cần mật khẩu, truy cập ít nhất một địa chỉ mạng chỉ định dựa vào địa chỉ mạng chỉ định; và xác định xem liệu mạng không dây được kết nối hiện tại

có cần xác minh đăng nhập thứ cấp hay không bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không.

Một cách tùy ý, bước xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không bao gồm các bước: gọi giao diện quản lý mật khẩu mạng không dây được cung cấp bởi hệ điều hành, thu kết quả gọi và xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không dựa vào kết quả gọi này.

Một cách tùy ý, địa chỉ mạng chỉ định bao gồm địa chỉ mạng của API (API – Application Program Interface – Giao diện chương trình ứng dụng) được định nghĩa bởi người dùng và API được sử dụng để trả về thông tin nhận dạng cụ thể khi API được truy cập; và bước xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không bao gồm các bước: thu kết quả truy cập của việc truy cập địa chỉ mạng của API và xác định xem liệu địa chỉ mạng của API có được truy cập thành công hay không dựa vào việc liệu kết quả truy cập có bao gồm thông tin nhận dạng cụ thể hay không.

Một cách tùy ý, địa chỉ mạng chỉ định bao gồm các địa chỉ mạng của ít nhất hai trang web khác nhau; và bước xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không bao gồm các bước: thu dữ liệu trang web được trả về sau khi địa chỉ mạng của mỗi trong số các trang web được truy cập và xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không bằng cách so sánh dữ liệu trang của các trang web, để xác định xem liệu địa chỉ mạng chỉ định của mỗi trong số các trang web có được truy cập thành công hay không.

Một cách tùy ý, dữ liệu trang của trang web bao gồm địa chỉ mạng của trang web; và bước xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không bằng cách so sánh dữ liệu trang của các trang web, bao gồm các bước: cập nhật dữ liệu trang của mỗi trong số các trang web, trong đó bước cập nhật này bao gồm việc xóa địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web hoặc thay thế địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web bằng dữ liệu nhận dạng thống nhất; và so sánh dữ liệu trang được cập nhật của các trang web để xác định xem liệu dữ liệu trang có

giống nhau hay không và xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không dựa vào kết quả so sánh.

Thiết bị phát hiện kiểu mạng không dây bao gồm: môđun xác định mật khẩu kết nối được tạo cấu hình để xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không; môđun truy cập được tạo cấu hình để: sau khi được xác định rằng không cần mật khẩu, truy cập ít nhất một địa chỉ mạng chỉ định dựa vào địa chỉ mạng chỉ định; và môđun xác minh đăng nhập được tạo cấu hình để xác định xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không, bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không.

Một cách tùy ý, môđun xác định mật khẩu kết nối còn được tạo cấu hình để: gọi giao diện quản lý mật khẩu mạng không dây được cung cấp bởi hệ điều hành, thu kết quả gọi và xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không dựa vào kết quả gọi này.

Một cách tùy ý, địa chỉ mạng chỉ định bao gồm địa chỉ mạng của API được định nghĩa bởi người dùng và API được sử dụng để trả về thông tin nhận dạng cụ thể khi API được truy cập; và môđun xác minh đăng nhập còn được tạo cấu hình để: thu kết quả truy cập của việc truy cập địa chỉ mạng API và xác định liệu địa chỉ mạng của API có được truy cập thành công hay không dựa vào việc liệu kết quả truy cập có bao gồm thông tin nhận dạng cụ thể hay không.

Một cách tùy ý, địa chỉ mạng chỉ định bao gồm các địa chỉ mạng của ít nhất hai trang web khác nhau; và môđun xác minh đăng nhập còn được tạo cấu hình để: thu dữ liệu trang web được trả về sau khi địa chỉ mạng của mỗi trong số các trang web được truy cập và xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không bằng cách so sánh dữ liệu trang của các trang web, để xác định xem liệu địa chỉ mạng chỉ định của mỗi trong số các trang web có được truy cập thành công hay không.

Một cách tùy ý, dữ liệu trang của trang web bao gồm địa chỉ mạng của trang web; và môđun xác minh đăng nhập còn được tạo cấu hình để: cập nhật dữ liệu trang của mỗi trong số các trang web, trong đó bước cập nhật bao gồm việc xóa địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web hoặc thay thế

địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web bằng dữ liệu nhận dạng thống nhất; và so sánh dữ liệu trang được cập nhật của các trang web để xác định xem liệu dữ liệu trang có giống nhau hay không và xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không dựa vào kết quả so sánh.

Thiết bị điện tử bao gồm: bộ xử lý; và bộ nhớ được tạo cấu hình để lưu trữ lệnh có thể được thực thi bởi bộ xử lý, trong đó bộ xử lý được tạo cấu hình để: xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không; sau khi xác định rằng không cần mật khẩu, truy cập ít nhất một địa chỉ mạng chỉ định dựa vào địa chỉ mạng chỉ định; và xác định xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không.

Các giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế có thể bao gồm các hiệu quả có lợi sau đây:

Theo phương pháp phát hiện kiểu mạng không dây trong sáng chế, sau khi xác định rằng mạng không dây được kết nối hiện tại không cần mật khẩu để kết nối, địa chỉ mạng chỉ định tiếp tục được truy cập. Việc xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không cũng được xác định. Nếu địa chỉ mạng có thể được truy cập, có thể xác định được rằng, mạng không dây được kết nối hiện tại là mạng không dây không có mật khẩu. Nếu địa chỉ mạng không thể được truy cập, có thể xác định được rằng, mạng không dây cần xác minh đăng nhập thứ cấp. Theo các phương án thực hiện của sáng chế, việc xác định xem liệu mạng không dây không có mật khẩu có cần xác minh đăng nhập thứ cấp để kết nối hay không có thể được xác định một cách chính xác. Do đó, người dùng có thể được cảnh báo một cách chính xác về rủi ro bảo mật mạng không dây, làm giảm tỉ lệ xác thực sai và sự gián đoạn với người dùng.

Cần hiểu rằng, phần mô tả tổng quát ở trên và phần mô tả chi tiết sau đây chỉ nhằm lấy ví dụ và minh họa và không nhằm giới hạn sáng chế.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo được bao gồm trong sáng chế cấu thành một phần của sáng chế, minh họa các phương án thích hợp với sáng chế và cùng với phần mô tả được sử dụng để giải thích các nguyên lý của sáng chế.

Fig.1 là sơ đồ minh họa việc kết nối với mạng không dây qua Wi-Fi bởi thiết bị điện tử theo một phương án làm ví dụ của sáng chế;

Fig.2A là lưu đồ minh họa phương pháp phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế;

Fig.2B là sơ đồ minh họa giải pháp phát hiện kiểu mạng không dây của thiết bị điện tử theo một phương án làm ví dụ của sáng chế;

Fig.2C là lưu đồ minh họa phương pháp phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế;

Fig.2D là lưu đồ minh họa phương pháp phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế;

Fig.3 là sơ đồ phân cứng theo kết cấu minh họa thiết bị điện tử bao gồm thiết bị phát hiện kiểu mạng không dây theo sáng chế;

Fig.4 là sơ đồ khối minh họa thiết bị phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế; và

Fig.5 là lưu đồ minh họa một ví dụ của phương pháp được thực hiện bằng máy tính để xác định kiểu mạng không dây theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Các phương án làm ví dụ được mô tả chi tiết ở đây và các ví dụ của các phương án làm ví dụ được minh họa trên các hình vẽ kèm theo. Khi phần mô tả sau đây tham chiếu đến các hình vẽ kèm theo, các số chỉ dẫn giống nhau trên các hình vẽ khác nhau chỉ các thành phần giống nhau hoặc tương tự trừ khi được nêu khác đi. Các phương án thực hiện được mô tả trong các phương án làm ví dụ sau đây không biểu diễn tất cả các phương án thích hợp với sáng chế. Thay vào đó, chúng chỉ là các ví dụ về thiết bị và các phương pháp thích hợp với một số khía cạnh của sáng chế như được nêu trong bộ yêu cầu bảo hộ kèm theo.

Các thuật ngữ được sử dụng trong sáng chế chỉ nhằm mục đích minh họa các phương án cụ thể và không nhằm giới hạn sáng chế. Các thuật ngữ dạng số ít được sử dụng trong sáng chế và các điểm yêu cầu bảo hộ kèm theo của sáng chế cũng nhằm bao gồm các dạng số nhiều, trừ khi ngữ cảnh có chỉ định khác. Cũng cần hiểu rằng, thuật ngữ "và/hoặc" được sử dụng trong bản mô tả này chỉ định và bao gồm các kết hợp có thể có bất kỳ hoặc tất cả của một hoặc nhiều mục được liệt kê liên quan.

Cần hiểu rằng, mặc dù các thuật ngữ như "thứ nhất", "thứ hai" và "thứ ba" được sử dụng trong sáng chế để mô tả các kiểu thông tin khác nhau, nhưng các thông tin đó không bị giới hạn bởi các thuật ngữ này. Các thuật ngữ này chỉ được sử dụng để phân biệt thông tin có cùng kiểu. Ví dụ, không nằm ngoài phạm vi của sáng chế, thông tin thứ nhất cũng có thể đề cập đến thông tin thứ hai và tương tự, thông tin thứ hai cũng có thể đề cập đến thông tin thứ nhất. Phụ thuộc vào ngữ cảnh, từ "nếu" như được sử dụng trong bản mô tả này có thể được hiểu là "khi" hoặc "trong trường hợp mà..." hoặc "để đáp lại việc xác định".

Theo các phương án của sáng chế, Wi-Fi là công nghệ cho phép thiết bị điện tử kết nối với mạng cục bộ không dây (WLAN) và cho phép các thiết bị đầu cuối như máy tính cá nhân và thiết bị cầm tay (ví dụ, PDA hoặc điện thoại di động) kết nối không dây với nhau.

Trạm phát Wi-Fi là thiết bị có thể cung cấp tài nguyên mạng chia sẻ và cho phép các thiết bị đầu cuối khác (ví dụ, điện thoại di động và/hoặc máy tính xách tay) kết nối với mạng qua sự kết nối Wi-Fi. Ví dụ, nếu kết nối mạng không dây có thể được thực hiện qua kết nối Wi-Fi trong vùng phủ sóng hiệu quả của sóng vô tuyến của bộ định tuyến không dây, thì bộ định tuyến không dây này được gọi là "trạm phát Wi-Fi".

Sự xác minh đăng nhập thứ cấp Wi-Fi: mặc dù mật khẩu không được yêu cầu khi thiết bị được kết nối với trạm phát Wi-Fi, khi truy cập Internet, màn hình đăng nhập vẫn sẽ hiện lên để yêu cầu người dùng nhập tên người dùng và mật khẩu. Phương pháp kết nối đăng nhập này được gọi là "xác thực đăng nhập thứ cấp Wi-Fi".

Fig.1 là sơ đồ minh họa việc kết nối với mạng không dây qua Wi-Fi bởi thiết bị điện tử theo một phương án làm ví dụ của sáng chế. Khi kết nối với trạm phát mạng không dây, thiết bị điện tử có thể truy cập mạng không dây không sử dụng mật khẩu. Tuy nhiên, người dùng cần nhập tên người dùng và mật khẩu khi thiết bị điện tử truy

cập Internet qua mạng không dây. Do đó, mạng không dây không phải là Wi-Fi không có mật khẩu theo thực tế.

Giải pháp phát hiện kiểu mạng không dây theo các phương án của sáng chế, sau khi xác định rằng mạng không dây được kết nối hiện tại không cần mật khẩu để kết nối, địa chỉ mạng được chỉ định có thể tiếp tục được truy cập. Việc liệu địa chỉ mạng chỉ định có được truy cập thành công hay không cũng được xác định. Nếu đúng, có thể xác định được rằng, mạng không dây được kết nối hiện tại là mạng không dây không có mật khẩu. Nếu không đúng, có thể xác định được rằng, mạng không dây này cần xác minh đăng nhập thứ cấp. Theo các phương án của sáng chế, việc liệu mạng không dây không có mật khẩu có cần xác minh đăng nhập thứ cấp để kết nối hay không có thể được xác định một cách chính xác. Do đó, người dùng có thể được cảnh báo một cách chính xác về rủi ro bảo mật không dây, làm giảm tỉ lệ xác thực sai và sự gián đoạn với người dùng. Phần sau đây sẽ mô tả chi tiết các phương án của sáng chế.

Fig.2A là lưu đồ minh họa phương pháp phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế. Phương pháp phát hiện kiểu mạng không dây này bao gồm các bước từ 202 đến 206 dưới đây.

Bước 202: Xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không.

Bước 204: Sau khi xác định rằng không cần mật khẩu, dựa vào ít nhất một địa chỉ mạng chỉ định, truy cập địa chỉ mạng chỉ định này.

Bước 206: Xác định xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không.

Phương pháp theo phương án này có thể được áp dụng cho thiết bị điện tử được tạo cấu hình có môđun mạng không dây. Ví dụ, phương pháp có thể được áp dụng cho ứng dụng được cài đặt trong thiết bị điện tử. Ứng dụng này có thể phát hiện kiểu mạng không dây mà thiết bị điện tử truy cập và cung cấp cảnh báo rủi ro bảo mật về mạng không dây cho người dùng dựa vào kiểu được phát hiện. Thiết bị điện tử theo phương án này có thể bao gồm điện thoại thông minh, máy tính bảng, thiết bị hỗ trợ kỹ thuật số cá nhân, trình đa phương tiện, v.v. Kiểu thiết bị điện tử này được tạo cấu hình có môđun mạng không dây và có thể truy cập mạng không dây. Fig.2B là sơ đồ minh họa

giải pháp phát hiện kiểu mạng không dây của thiết bị điện tử theo một phương án làm ví dụ của sáng chế.

Khi thiết bị điện tử kết nối với mạng không dây được cung cấp bởi bộ định tuyến, thiết bị cổng nối hoặc thiết bị đầu cuối mạng khác, ứng dụng có thể xác định rằng, thiết bị điện tử kết nối với mạng không dây theo nhiều cách khác nhau và xác định xem liệu có cần mật khẩu để truy cập hay không. Ví dụ, nếu chương trình ứng dụng có sự cho phép, thiết bị điện tử có thể xác định rằng thiết bị điện tử có sự truy cập vào trạm phát Wi-Fi mạng không dây bằng cách truyền thông trực tiếp với môđun mạng không dây hoặc bằng cách đọc giao diện được cung cấp bởi môđun mạng không dây hoặc bằng cách sử dụng phương pháp khác. Chương trình ứng dụng cũng có thể xác định xem liệu trạm phát Wi-Fi mạng không dây được truy cập có cần mật khẩu để kết nối hay không. Theo một ví dụ khác, chương trình ứng dụng có thể có sự cho phép và hệ điều hành của thiết bị điện tử cung cấp giao diện, chương trình ứng dụng này có thể đưa ra các quyết định dựa vào kết quả gọi của lời gọi giao diện. Trong ứng dụng thực tế, chương trình ứng dụng có thể xác định một cách linh hoạt dựa vào một số yếu tố như là hệ điều hành được sử dụng bởi thiết bị điện tử, sự cho phép của hệ điều hành mà nhà cung cấp ứng dụng có thể thu và giao diện được cung cấp bởi hệ điều hành.

Theo phương pháp của phương án thực hiện tùy ý, bước xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không bao gồm các bước: gọi giao diện quản lý mật khẩu mạng không dây được cung cấp bởi hệ điều hành, thu kết quả gọi và xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không dựa vào kết quả gọi này.

Lấy hệ điều hành Android làm ví dụ, hệ điều hành này cung cấp giao diện quản lý mật khẩu mạng không dây cho môđun mạng không dây. Ứng dụng có thể gọi giao diện và xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không dựa vào kết quả gọi của lời gọi giao diện. Phần mô tả dưới đây minh họa mã để gọi giao diện quản lý mật khẩu mạng không dây:

/**

* Xác định xem liệu Wi-Fi được kết nối hiện tại có cần mật khẩu để truy cập hay không bằng cách sử dụng cấu hình quản lý WiFiConfiguration.KeyMgmt.

*

*@return true: yêu cầu mật khẩu để truy cập, false: không cần mật khẩu để truy cập

*/

```
public static boolean needPassword(Context context) {
    WiFiManager wifiManager = (WiFiManager)
context.getSystemService(Context.WIFI_SERVICE);

    if (wifiManager != null) {
        List<WiFiConfiguration> configurations =
WiFiManager.getConfiguredNetworks();

        if (configurations != null && configurations.size() > 0) {
            for (WiFiConfiguration configuration : configurations) {
                if
(configuration != null && configuration.status ==
WiFiConfiguration.Status.CURRENT) {
                    if
(configuration.allowedKeyManagement.get(WiFiConfiguration.KeyMgmt.NONE)) {
                        return false;
                    } else {
                        return true;
                    }
                }
            }
        }
    }
}

//Mật khẩu kết nối cần thiết theo mặc định.
```

```
return true;
```

```
}
```

WiFiManager.getConfiguredNetworks() biểu diễn giao diện quản lý mật khẩu mạng không dây.

Logic chính của mã là để phát hiện: xem liệu WiFiConfiguration.allowedKeyManagement của trạm phát Wi-Fi có bao gồm trường WiFiConfiguration.keyMgmt.NONE hay không. Nếu đúng, được xem là không cần mật khẩu; hoặc nếu không đúng, được xem là mật khẩu là cần thiết. Khi mật khẩu không được yêu cầu để kết nối mạng không dây, kết quả gọi bao gồm trường KeyMgmt.NONE.

Lấy hệ điều hành iOS làm ví dụ, hệ điều hành iOS này cung cấp API (được gọi là NEHotspotNetwork) để thu danh sách Wi-Fi chủ yếu thông qua các bước sau đây: yêu cầu Apple cho phép triển khai tiện ích mở rộng mạng, áp dụng đối với tệp tin mô tả bao gồm tiện ích mở rộng mạng, tạo cấu hình Info.plist, tạo cấu hình các quyền, thu sự thực hiện mã danh sách Wi-Fi nhờ iOS và thu lời gọi lại danh sách Wi-Fi.

Sau khi NEHotspotNetwork được gọi, thông tin trả về của NEHotspotNetwork bao gồm: SSID: tên Wi-Fi, BSSID: địa chỉ MAC của vị trí; signalStrength: cường độ tín hiệu Wi-Fi, có giá trị nằm trong khoảng 0,0–1,0; bảo mật: chỉ báo xem liệu mạng có bảo mật hay không (giá trị là sai đối với Wi-Fi không cần mật khẩu để truy cập); autoJoined: chỉ báo xem liệu thiết bị có kết nối tự động với Wi-Fi hay không; justJoined: chỉ báo xem liệu mạng có vừa được truy cập hay không; và chosenHelper: chỉ báo xem liệu HotspotHelper có được lựa chọn cho mạng hay không.

Do đó, dựa vào tính bảo mật theo kết quả gọi, có thể được xác định xem liệu trạm phát Wi-Fi mạng không dây được kết nối hiện tại có cần có mật khẩu hay không.

Tuy nhiên, sau khi truy cập mạng không dây mà không sử dụng mật khẩu, một số mạng vẫn yêu cầu người dùng xác minh đăng nhập thứ cấp. Do đó, theo phương án này, việc xác định xem liệu có cần xác minh đăng nhập thứ cấp hay không được xác định bằng cách chỉ định trước một hoặc nhiều địa chỉ mạng và truy cập vào địa chỉ mạng đã chỉ định. Giả định rằng, việc xác minh đăng nhập thứ cấp là cần thiết, người dùng chỉ có thể truy cập Internet sau khi nhập tên tài khoản và mật khẩu. Nếu người

dùng không thực hiện xác minh đăng nhập thứ cấp, thiết bị điện tử không thể thu được dữ liệu mạng mong muốn sau khi truy cập Internet. Trên cơ sở đó, theo phương án này, một hoặc nhiều địa chỉ mạng được chỉ định và địa chỉ mạng đã chỉ định này được truy cập. Nếu địa chỉ mạng chỉ định được truy cập thành công, điều này chỉ báo rằng mạng không dây được truy cập không cần xác minh đăng nhập thứ cấp. Nếu địa chỉ mạng chỉ định truy cập không thành công, thì mạng không dây được truy cập yêu cầu xác minh đăng nhập thứ cấp.

Trong sử dụng thực tế, việc xác định xem liệu truy cập có thành công hay không có thể được thực hiện theo nhiều cách. Ví dụ, dữ liệu mạng tương ứng với địa chỉ mạng chỉ định có thể được tạo cấu hình trước. Sau khi địa chỉ mạng chỉ định được truy cập, kết quả truy cập được thu và xác định xem liệu truy cập có thành công hay không được thực hiện dựa vào việc liệu kết quả truy cập có giống với dữ liệu mạng được tạo cấu hình trước hay không.

Theo phương án này, địa chỉ mạng chỉ định bao gồm địa chỉ mạng của API được định nghĩa bởi người dùng và API này được sử dụng để trả về thông tin nhận dạng cụ thể khi được truy cập.

Bước xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không bao gồm các bước: thu kết quả truy cập của việc truy cập địa chỉ mạng của API và xác định dựa vào việc liệu kết quả truy cập có bao gồm thông tin nhận dạng cụ thể hay không, liệu địa chỉ mạng của API có được truy cập thành công hay không.

Theo phương án này, API có thể được triển khai trên máy chủ trước. Ứng dụng có thể truy cập địa chỉ mạng của API và địa chỉ mạng có thể là địa chỉ IP. Nếu mạng là tiếp cận được, thông tin nhận dạng cụ thể có thể thu được sau khi API được truy cập. Nếu mạng là không tiếp cận được, thông tin nhận dạng cụ thể không thể thu được. Như vậy, có thể được xác định xem liệu địa chỉ mạng của API có được truy cập thành công hay không và liệu xác minh đăng nhập thứ cấp có cần thiết hay không.

Theo một số ví dụ khác, công việc triển khai trước có thể không được thực hiện. Địa chỉ mạng có thể là địa chỉ mạng của trang web công cộng. Nội dung trang của trang web này có thể được phân tích trước và được lưu trữ trước. Việc kết quả truy cập của việc truy cập trang web có bao gồm nội dung trang được lưu trữ trước hay không được xác định, để xác định xem liệu việc truy cập có thành công hay không. Tuy

nhiên, nội dung trang web có thể thay đổi động. Do đó, theo phương án này, các địa chỉ mạng của hai hoặc nhiều trang web có thể được chỉ định, để cung cấp phương pháp xác định đáng tin cậy hơn. Cụ thể là, sáng chế đề xuất phương án sau đây.

Địa chỉ mạng chỉ định bao gồm các địa chỉ mạng của ít nhất hai trang web khác nhau; và việc xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không bao gồm các bước: thu dữ liệu trang web được trả về sau khi địa chỉ mạng của mỗi trong số các trang web được truy cập và xác định bằng cách so sánh dữ liệu trang của các trang web, xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không, để xác định xem liệu địa chỉ mạng chỉ định của trang web có được truy cập thành công hay không.

Hai hoặc nhiều trang web công cộng hiện có hoặc các trang web với nội dung trang tương đối đơn giản có thể được lựa chọn làm các trang web được nêu trên, để làm giảm sự tiêu thụ lưu lượng dữ liệu. Địa chỉ mạng có thể bao gồm địa chỉ tên miền hoặc địa chỉ IP của trang web. Nếu mạng là không tiếp cận được, thì mỗi trang web được truy cập chuyển đến trang xác minh đăng nhập thứ cấp. Trong trường hợp này, dữ liệu trang của trang xác minh đăng nhập thứ cấp được trả về và dữ liệu trang được trả về này về cơ bản là giống nhau. Nếu mạng là tiếp cận được, sau khi hai hoặc nhiều trang web được truy cập, dữ liệu trang của mỗi trang web được trả về và dữ liệu trang của mỗi trang web là khác nhau. Do đó, theo phương án này, có thể được xác định bằng cách so sánh dữ liệu trang của các trang web, xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không, để xác định xem liệu địa chỉ mạng chỉ định của của mỗi trong số các trang web có được truy cập thành công hay không.

Sau khi việc truy cập vào địa chỉ mạng được bắt đầu, có thể thu được dữ liệu trang được trả về từ địa chỉ mạng. Dữ liệu trang này bao gồm địa chỉ mạng của trang web. Nếu mạng là không tiếp cận được, dữ liệu trang được trả về bao gồm dữ liệu trang của trang xác minh đăng nhập thứ cấp. Trong trường hợp này, tất cả dữ liệu trang là giống nhau ngoại trừ địa chỉ mạng. Trên cơ sở đó, theo phương án này, để cải thiện hiệu suất và độ chính xác của bước xác định, việc xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không bằng cách so sánh dữ liệu trang của các trang web, bao gồm các bước: cập nhật dữ liệu trang của mỗi trong số các trang web, trong đó bước cập nhật bao gồm việc xóa địa chỉ mạng

được bao gồm trong dữ liệu trang của mỗi trong số các trang web hoặc thay thế địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web bằng dữ liệu nhận dạng thống nhất; và so sánh dữ liệu trang được cập nhật của các trang web để xác định xem liệu dữ liệu trang có giống nhau hay không và xác định dựa vào kết quả so sánh, xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không.

Theo phương án này, sau khi các địa chỉ mạng trong dữ liệu trang được xóa hoặc được thay thế bằng dữ liệu nhận dạng thống nhất, dữ liệu trang được cập nhật của các trang web được so sánh để xác định xem liệu dữ liệu trang được cập nhật có giống nhau hay không. Do đó, hiệu quả và độ chính xác của việc so sánh có thể được cải thiện một cách đáng kể.

Phần sau đây sẽ mô tả chi tiết sáng chế bằng cách sử dụng hai phương án.

Fig.2C là lưu đồ minh họa phương pháp phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế. Trên Fig.2C, hệ điều hành Android được sử dụng làm ví dụ. Giao diện quản lý mật khẩu mạng không dây của hệ điều hành, nghĩa là, `WiFiManager.getConfiguredNetworks()`, được gọi và bước xác định được thực hiện dựa vào việc liệu kết quả gọi có bao gồm trường `WiFiConfiguration.keyMgmt.NONE` hay không. Nếu không, mật khẩu được xem là cần thiết và kết quả xác định được trả về ngay lập tức. Nếu là đúng, có thể tiếp tục xác định xem liệu trạm phát Wi-Fi mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không.

Một cách cụ thể, API có thể được triển khai trên máy chủ riêng và API được sử dụng để trả về cờ thành công đơn giản. Ứng dụng truy cập trực tiếp API. Nếu nhận được cờ thành công, ứng dụng được xem là có thể truy cập một cách trực tiếp Internet qua trạm phát Wi-Fi mạng không dây được kết nối hiện tại và việc xác minh đăng nhập thứ cấp là không cần thiết. Nếu không, việc xác minh đăng nhập thứ cấp được xem là cần thiết.

Fig.2D là lưu đồ minh họa phương pháp phát hiện kiểu mạng không dây khác theo một phương án làm ví dụ của sáng chế. Trên Fig.2D, hệ điều hành Android được sử dụng làm ví dụ. Giao diện quản lý mật khẩu mạng không dây của hệ điều hành, nghĩa là `WiFiManager.getConfiguredNetworks()`, được gọi và bước xác định được thực hiện dựa vào việc liệu kết quả gọi có bao gồm trường

WiFiConfiguration.keyMgmt.NONE hay không. Nếu không, mật khẩu được xem là cần thiết và kết quả xác định được trả về ngay lập tức. Nếu đúng, có thể tiếp tục xác định xem liệu trạm phát Wi-Fi mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không.

Một cách cụ thể, so sánh với việc triển khai API trên máy chủ riêng trên Fig.2C, theo phương án này, các địa chỉ của hai website đơn giản đã biết (các website có thể càng đơn giản càng tốt để làm giảm sự tiêu thụ lưu lượng dữ liệu) có thể được lựa chọn. Giả định rằng, các website là website A (địa chỉ website là url_A) và website B (địa chỉ website là url_B), các địa chỉ các website url_A và url_B được truy cập theo thứ tự và dữ liệu tương ứng được trả về từ các địa chỉ được lưu trữ trong các bản ghi tương ứng: response_A và response_B. Cuối cùng, nội dung của response_A và response_B được so sánh.

Nếu trạm phát Wi-Fi mạng không dây được kết nối hiện tại cần xác minh đăng nhập thứ cấp, các địa chỉ website được truy cập url_A và url_B đều chuyển đến trang xác minh đăng nhập thứ cấp, nghĩa là, nội dung của response_A và response_B đều bao gồm dữ liệu trang của cùng trang xác minh đăng nhập thứ cấp. Mặt khác, response_A và response_B biểu diễn nội dung của các website khác nhau và chắc chắn là khác nhau. Do đó, có thể được xác định xem liệu Wi-Fi hiện tại có cần xác minh đăng nhập thứ cấp hay không.

Tuy nhiên, do response_A và response_B bao gồm địa chỉ mạng tương ứng, địa chỉ mạng có thể được thay thế bằng dữ liệu nhận dạng thống nhất trước khi so sánh giữa response_A và response_B. Theo phương án này, địa chỉ mạng được thay thế bởi url_B. Do đó, response_A.replace("url_A", "url_B") có thể được thực thi, nghĩa là, địa chỉ mạng trong response_A được thay thế bởi url_B, để loại trừ sự khác nhau về địa chỉ mạng trong dữ liệu trang, nhờ đó tránh được sự đánh giá sai và làm tăng hiệu quả và độ chính xác của việc xác định.

Tương ứng với phương án nêu trên của phương pháp phát hiện kiểu mạng không dây, sáng chế còn đề xuất các phương án của thiết bị phát hiện kiểu mạng không dây và thiết bị điện tử mà thiết bị phát hiện kiểu mạng không dây được áp dụng.

Phương án của thiết bị phát hiện kiểu mạng không dây theo sáng chế có thể được áp dụng cho thiết bị điện tử. Phương án thiết bị có thể được thực hiện bằng cách

sử dụng phần cứng, phần mềm hoặc kết hợp của phần cứng và phần mềm. Ví dụ, khi thực hiện bằng phần mềm, thiết bị phát hiện kiểu mạng không dây là thiết bị logic và được tạo ra khi bộ xử lý phát hiện kiểu mạng không dây của thiết bị phát hiện kiểu mạng không dây đọc lệnh chương trình máy tính tương ứng trong bộ nhớ không khả biến và thực thi lệnh chương trình máy tính trong bộ nhớ. Theo khía cạnh phần cứng, Fig.3 là sơ đồ phần cứng theo kết cấu minh họa thiết bị điện tử bao gồm thiết bị phát hiện kiểu mạng không dây theo sáng chế. Ngoài bộ xử lý 310, bộ nhớ 330, giao diện mạng 320 và bộ nhớ không khả biến 340 được thể hiện trên Fig.3, theo phương án này, thiết bị điện tử trong đó thiết bị 331 được định vị thường có thể còn bao gồm phần cứng khác dựa vào chức năng thực tế của thiết bị điện toán. Các chi tiết sẽ không được lặp lại ở đây.

Fig.4 là sơ đồ khối minh họa thiết bị phát hiện kiểu mạng không dây theo một phương án làm ví dụ của sáng chế. Thiết bị này bao gồm: môđun xác định mật khẩu kết nối 41, được tạo cấu hình để xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không; môđun truy cập 42, được tạo cấu hình để: sau khi xác định rằng không cần mật khẩu, truy cập ít nhất một địa chỉ mạng chỉ định dựa vào địa chỉ mạng chỉ định; và môđun xác minh đăng nhập 43, được tạo cấu hình để xác định bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không, xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không.

Một cách tùy ý, môđun xác định mật khẩu kết nối còn được tạo cấu hình để: gọi giao diện quản lý mật khẩu mạng không dây được cung cấp bởi hệ điều hành, thu kết quả gọi và xác định dựa vào kết quả gọi này, xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không.

Một cách tùy ý, địa chỉ mạng chỉ định bao gồm địa chỉ mạng của API được định nghĩa bởi người dùng và API được sử dụng để trả về thông tin nhận dạng cụ thể khi API được truy cập; và môđun xác minh đăng nhập còn được tạo cấu hình để: thu kết quả truy cập của bước truy cập địa chỉ mạng của API và xác định dựa vào việc liệu kết quả truy cập có bao gồm thông tin nhận dạng cụ thể hay không, liệu địa chỉ mạng của API có được truy cập thành công hay không.

Một cách tùy ý, địa chỉ mạng chỉ định bao gồm các địa chỉ mạng của ít nhất hai trang web khác nhau; và môđun xác minh đăng nhập còn được tạo cấu hình để: thu dữ liệu trang web được trả về sau khi địa chỉ mạng của mỗi trong số các trang web được truy cập và xác định bằng cách so sánh dữ liệu trang của các trang web, xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không, để xác định xem liệu địa chỉ mạng chỉ định của của mỗi trong số các trang web có được truy cập thành công hay không.

Một cách tùy ý, dữ liệu trang của trang web bao gồm địa chỉ mạng của trang web; và môđun xác minh đăng nhập còn được tạo cấu hình để: cập nhật dữ liệu trang của mỗi trong số các trang web, trong đó bước cập nhật bao gồm việc xóa địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web hoặc thay thế địa chỉ mạng được bao gồm trong dữ liệu trang của mỗi trong số các trang web bằng dữ liệu nhận dạng thống nhất; và so sánh dữ liệu trang được cập nhật của các trang web để xác định xem liệu dữ liệu trang có giống nhau hay không và xác định dựa vào kết quả so sánh, xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không.

Thiết bị điện tử bao gồm: bộ xử lý; và bộ nhớ, được tạo cấu hình để lưu trữ lệnh mà có thể được thực thi bởi bộ xử lý, trong đó bộ xử lý được tạo cấu hình để: xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không; sau khi xác định rằng không cần mật khẩu, truy cập ít nhất một địa chỉ mạng chỉ định dựa vào địa chỉ mạng chỉ định; và xác định xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không bằng cách xác định xem liệu địa chỉ mạng chỉ định có được truy cập thành công hay không.

Đối với các chi tiết về các quy trình thực hiện các chức năng và các mục đích của các môđun trong thiết bị, tham chiếu đến các quy trình thực hiện của các bước tương ứng theo phương pháp và các chi tiết sẽ không được lặp lại ở đây.

Phương án thiết bị về cơ bản tương ứng với phương án phương pháp; do đó, đối với các phần liên quan, tham chiếu đến các phần mô tả từng phần theo phương án phương pháp. Phương án thiết bị được mô tả chỉ là ví dụ. Các môđun được mô tả là các phần riêng biệt có thể hoặc không thể riêng biệt về mặt vật lý và các phần được hiển thị là các môđun có thể hoặc không thể là các môđun vật lý, nghĩa là có thể được

định vị tại một vị trí hoặc có thể được phân tán trên nhiều mô đun mạng. Một số hoặc tất cả các mô đun có thể được lựa chọn dựa vào các yêu cầu thực tế để đạt được các mục đích của các giải pháp sáng chế. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật này có thể hiểu và thực hiện các phương án của sáng chế mà không cần nỗ lực sáng tạo.

Các phương án cụ thể của sáng chế được mô tả ở trên. Các phương án khác thuộc phạm vi của bộ yêu cầu bảo hộ kèm theo. Trong một số trường hợp, các hoạt động hoặc các bước được nêu trong các điểm yêu cầu bảo hộ có thể được thực hiện theo thứ tự khác với thứ tự trong các phương án mà vẫn đạt được các kết quả mong muốn. Ngoài ra, các quy trình được minh họa trên các hình vẽ kèm theo không nhất thiết yêu cầu thứ tự được minh họa cụ thể hoặc thứ tự liên tiếp để đạt được các kết quả mong muốn. Theo các phương án nhất định, xử lý đa nhiệm và song song cũng có thể được áp dụng hoặc có thể tạo ra lợi thế.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ dễ dàng thừa nhận các phương án khác của sáng chế khi xem xét sáng chế và việc thực hiện sáng chế như được áp dụng ở đây. Sáng chế bao gồm sự biến đổi, sử dụng hoặc sự điều chỉnh bất kỳ của sáng chế để phù hợp với các nguyên lý tổng quát của sáng chế và bao gồm kiến thức tổng quát chung hoặc các phương tiện kỹ thuật trong lĩnh vực mà không được bảo hộ trong sáng chế. Sáng chế và các phương án chỉ được xem là các ví dụ, với phạm vi và bản chất thực của sáng chế được chỉ báo bởi các điểm yêu cầu bảo hộ sau đây.

Cần hiểu rằng, sáng chế không bị giới hạn bởi các kết cấu chính xác như được mô tả ở trên và được thể hiện trên các hình vẽ kèm theo và các phương án cải biến và các thay đổi khác nhau có thể được thực hiện mà không nằm ngoài phạm vi của sáng chế. Phạm vi của sáng chế chỉ bị giới hạn bởi bộ yêu cầu bảo hộ kèm theo.

Phần mô tả ở trên chỉ là các ví dụ được ưu tiên của các phương án của sáng chế, mà không nhằm giới hạn sáng chế. Các phương án cải biến bất kỳ, các thay thế tương đương và cải tiến được tiến hành mà không nằm ngoài tinh thần và nguyên lý của sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế.

Fig.5 là lưu đồ minh họa ví dụ của phương pháp được thực hiện bằng máy tính 500 để xác định kiểu mạng không dây, theo một phương án thực hiện của sáng chế. Để làm rõ vấn đề này, phần mô tả sau đây mô tả tổng quát phương pháp 500 theo ngữ

cảnh của các hình vẽ khác trong phần mô tả này. Tuy nhiên, cần hiểu rằng, phương pháp 500 có thể được thực hiện, ví dụ, bởi hệ thống, môi trường, phần mềm và phần cứng bất kỳ hoặc kết hợp của hệ thống, môi trường, phần mềm và phần cứng, miễn là thích hợp. Theo một số phương án thực hiện, các bước khác nhau của phương pháp 500 có thể được chạy song song, theo sự kết hợp, theo vòng lặp hoặc theo thứ tự bất kỳ.

Ở bước 505, bước xác định được thực hiện để xem liệu có cần mật khẩu để kết nối mạng không dây hay không. Theo một số phương án thực hiện, bước xác định được thực hiện tự động bởi thiết bị di động (như là điện thoại di động, máy tính xách tay) khi kết nối với mạng không dây. Mạng không dây có thể là mạng cục bộ không dây (WLAN). Trạm phát Wi-Fi (như bộ định tuyến không dây) có thể tạo kết nối Wi-Fi với WLAN khi thiết bị di động ở trong vùng phủ sóng của trạm phát Wi-Fi. Ví dụ, người dùng có thể lựa chọn trạm phát Wi-Fi trên thiết bị di động để bắt đầu kết nối Wi-Fi với WLAN. Theo một số phương án thực hiện, thiết bị di động có thể khởi động một cách tự động kết nối Wi-Fi với WLAN khi phát hiện trạm phát Wi-Fi. Khi được yêu cầu, trạm phát Wi-Fi có thể yêu cầu thiết bị di động cung cấp mật khẩu để kết nối thiết bị di động với WLAN. Theo một số phương án thực hiện, trạm phát Wi-Fi có thể kết nối thiết bị di động với WLAN không cần mật khẩu từ thiết bị di động.

Theo một số phương án thực hiện, để đáp lại việc xác định rằng mật khẩu là cần thiết để kết nối với mạng không dây, việc xác định được thực hiện mà sự kết nối đến mạng không dây là kết nối bảo mật. Trong trường hợp này, người dùng có thể nhập mật khẩu vào thiết bị di động để kết nối với mạng không dây. Nếu thiết bị di động có mật khẩu được lưu trữ cho mạng không dây, thì thiết bị di động này có thể cung cấp mật khẩu một cách tự động để kết nối với mạng không dây. Do kết nối với mạng không dây được xác định là kết nối bảo mật, không có rủi ro bảo mật về kết nối được hiển thị trên thiết bị di động và kết nối với mạng không dây không được chặn bởi, ví dụ, ứng dụng bảo mật trên thiết bị di động.

Theo một số phương án thực hiện, để xác định xem liệu có cần mật khẩu để kết nối với mạng không dây hay không, thiết bị di động có thể gọi, ví dụ giao diện quản lý mật khẩu mạng không dây được cung cấp bởi hệ điều hành của thiết bị di động. Thiết bị di động có thể thu kết quả gọi để đáp lại lời gọi giao diện quản lý mật khẩu mạng không dây. Sau đó, thiết bị di động có thể xác định xem liệu có cần mật khẩu để kết

nối với mạng không dây hay không dựa vào, ít nhất kết quả gọi. Ví dụ, nếu hệ điều hành là hệ điều hành Android, `WiFiManager.getConfiguredNetworks()` có thể là giao diện quản lý mật khẩu mạng không dây trong hệ điều hành Android này. Thiết bị di động có thể gọi giao diện này. Dựa vào, ít nhất kết quả gọi, thiết bị di động có thể xác định xem liệu `WiFiConfiguration.allowedKeyManagement` của trạm phát Wi-Fi của mạng không dây có bao gồm trường `WiFiConfiguration.keyMgmt.NONE` hay không. Nếu bao gồm trường này, thiết bị di động có thể xác định rằng không cần mật khẩu để kết nối với mạng không dây. Tuy nhiên, nếu không bao gồm trường này, thiết bị di động có thể xác định rằng mật khẩu là cần thiết để kết nối với mạng không dây. Nếu hệ điều hành là hệ điều hành là Apple iOS, `NEHotspotNetwork` có thể là giao diện chương trình ứng dụng (API) trong hệ điều hành Apple iOS. Thiết bị di động có thể gọi API. Dựa vào, ít nhất, chỉ báo bảo mật trong kết quả gọi, thiết bị di động có thể xác định xem liệu có cần mật khẩu để kết nối với mạng không dây hay không. Từ bước 505, phương pháp 500 tiến hành đến bước 510.

Ở bước 510, để đáp lại việc xác định rằng không cần mật khẩu để kết nối với mạng không dây, dữ liệu được truy hồi từ ít nhất một địa chỉ mạng định trước qua mạng không dây. Theo một số phương án thực hiện, dữ liệu được truy hồi tự động từ ít nhất một địa chỉ mạng định trước qua mạng không dây để đáp lại việc xác định. Ví dụ, đối với các ứng dụng khách hàng doanh nghiệp, API được định nghĩa bởi người dùng có thể được triển khai trên máy chủ riêng của doanh nghiệp. Ít nhất một địa chỉ mạng định trước có thể bao gồm địa chỉ mạng được kết hợp với API được định nghĩa bởi người dùng. API này có thể được tạo cấu hình để trả về thông tin nhận dạng cụ thể (như là ký hiệu nhận dạng “thành công”) khi API được truy cập. Đối với các ứng dụng khách hàng cá nhân, ít nhất hai địa chỉ mạng, mỗi địa chỉ được kết nối với trang web khác, có thể được định trước. Mỗi trang web có thể là trang web công cộng đã biết hiện có. Theo một số phương án thực hiện, để làm giảm lưu lượng dữ liệu, các trang web với nội dung trang đơn giản có thể được sử dụng để lựa chọn các địa chỉ mạng được định trước. Từ bước 510, phương pháp 500 tiến hành đến bước 515.

Ở bước 515, việc xác định được thực hiện để xem liệu việc xác minh đăng nhập thứ cấp có cần thiết để kết nối với mạng không dây hay không. Việc xác định được thực hiện dựa vào, ít nhất, dữ liệu được truy hồi từ ít nhất một địa chỉ mạng định trước. Theo một số phương án thực hiện, việc xác định được thực hiện một cách tự động bởi

thiết bị di động. Theo một số phương án thực hiện, mặc dù thiết bị di động không cần mật khẩu để kết nối với trạm phát Wi-Fi của mạng không dây ở bước 505, việc xác minh đăng nhập thứ cấp có thể có khi thiết bị di động truy cập Internet qua mạng không dây. Ví dụ, màn hình đăng nhập, yêu cầu tên người dùng, mật khẩu hoặc kết hợp của cả hai, có thể hiện lên thiết bị di động khi thiết bị di động này truy cập Internet qua mạng không dây. Trong một số trường hợp, trạm phát Wi-Fi của mạng không dây có thể đổi hướng yêu cầu truy cập đến trang xác minh đăng nhập thứ cấp, thay thế ít nhất một địa chỉ mạng định trước, nếu sự xác minh đăng nhập thứ cấp là cần thiết để kết nối với mạng không dây. Theo một số phương án thực hiện, trạm phát Wi-Fi có thể chuyển yêu cầu truy cập đến ít nhất một địa chỉ mạng định trước qua mạng không dây mà không cần xác minh đăng nhập thứ cấp từ thiết bị di động.

Theo một số phương án thực hiện, khi ít nhất một địa chỉ mạng định trước bao gồm địa chỉ mạng được kết hợp với API được định nghĩa bởi người dùng, thiết bị di động có thể truy cập địa chỉ mạng được kết hợp với API được định nghĩa bởi người dùng qua mạng không dây. Thiết bị di động này có thể thu phản hồi mạng đối với việc truy cập địa chỉ mạng được kết hợp với API được định nghĩa bởi người dùng qua mạng không dây thu được. Sau đó, thiết bị di động có thể xác định xem liệu việc xác minh đăng nhập thứ cấp có cần thiết để kết nối với mạng không dây hay không. Việc xác định được thực hiện dựa vào ít nhất, xem liệu phản hồi mạng thu được có bao gồm thông tin nhận dạng cụ thể hay không.

Ví dụ, nếu phản hồi mạng bao gồm ký hiệu nhận dạng “thành công”, thiết bị di động có thể xác định rằng yêu cầu truy cập đã tiếp cận địa chỉ mạng được kết hợp với API được định nghĩa bởi người dùng mà không cần xác minh đăng nhập thứ cấp. Do đó, việc xác định có thể được thực hiện nhờ thiết bị di động mà không cần xác minh đăng nhập thứ cấp để kết nối với mạng không dây. Tuy nhiên, nếu phản hồi mạng không bao gồm ký hiệu nhận dạng “thành công”, thiết bị di động có thể xác định rằng yêu cầu truy cập đã không tiếp cận được địa chỉ mạng được kết hợp với API được định nghĩa bởi người dùng mà không cần xác minh đăng nhập thứ cấp. Do đó, việc xác định có thể được thực hiện bởi thiết bị di động mà cần xác minh đăng nhập thứ cấp để kết nối với mạng không dây.

Theo một số phương án thực hiện, khi ít nhất một địa chỉ mạng định trước bao gồm ít nhất hai địa chỉ mạng được kết nối với các trang web khác nhau, thiết bị di

động có thể truy cập mỗi địa chỉ mạng trong số ít nhất hai địa chỉ mạng được kết hợp với các trang web khác nhau. Đối với mỗi địa chỉ mạng được truy cập, thu được dữ liệu trang web, bao gồm dữ liệu trang web thứ nhất được kết hợp với một trong số ít nhất hai địa chỉ mạng và dữ liệu trang web thứ hai được kết hợp với một địa chỉ khác trong số ít nhất hai địa chỉ mạng. Sau đó, dữ liệu trang web thứ nhất được so sánh với dữ liệu trang web thứ hai để xác định xem liệu dữ liệu trang web thứ nhất có khớp với dữ liệu trang web thứ hai hay không. Để đáp lại việc xác định rằng dữ liệu trang web thứ nhất khớp với dữ liệu trang web thứ hai, thiết bị di động có thể xác định rằng, việc xác minh đăng nhập thứ cấp là cần thiết để kết nối với mạng không dây.

Ví dụ, nếu các website A và B, lần lượt có các địa chỉ web URL_A và URL_B, được truy cập, dữ liệu trang web được trả về, lần lượt là response_A và response_B được thu và so sánh. Nếu response_A và response_B là khác nhau, thiết bị di động có thể xác định rằng yêu cầu truy cập đã tiếp cận cả hai website A và B mà không cần xác minh đăng nhập thứ cấp. Do đó, việc xác định có thể được thực hiện nhờ thiết bị di động mà không cần xác minh đăng nhập thứ cấp để kết nối với mạng không dây. Tuy nhiên, nếu response_A và response_B là giống nhau, thiết bị di động có thể xác định rằng yêu cầu truy cập không tiếp cận được website A hoặc B mà không cần xác minh đăng nhập thứ cấp. Ví dụ, yêu cầu truy cập đến cả hai website A và B được đổi hướng đến cùng trang xác minh đăng nhập thứ cấp và kết quả là response_A và response_B biểu diễn cùng nội dung của trang xác minh đăng nhập thứ cấp. Do đó, việc xác định có thể được thực hiện nhờ thiết bị di động mà việc xác minh đăng nhập thứ cấp là cần thiết để kết nối với mạng không dây.

Theo một số phương án thực hiện, việc so sánh dữ liệu trang web thứ nhất với dữ liệu trang web thứ hai có thể bao gồm việc cập nhật dữ liệu trang web thứ nhất và dữ liệu trang web thứ hai để loại bỏ dữ liệu địa chỉ mạng tương ứng hoặc thay thế dữ liệu địa chỉ mạng tương ứng bằng dữ liệu nhận dạng thống nhất và so sánh dữ liệu trang web thứ nhất được cập nhật với dữ liệu trang web thứ hai được cập nhật. Ví dụ, nếu response_A bao gồm URL_A và response_B bao gồm URL_B, việc so sánh response_A và response_B sẽ là khác nhau nếu URL_A và URL_A là khác nhau, ngay cả khi việc xác minh đăng nhập thứ cấp là cần thiết để kết nối với mạng không dây. Trong trường hợp này, URL_A trong response_A và URL_B trong response_B có thể được xóa trước khi so sánh. Theo một số phương án thực hiện, URL_A trong

response_A và URL_B trong response_B có thể được thay thế bằng cùng địa chỉ web trước khi so sánh. Ví dụ, URL_A trong response_A có thể được thay thế bằng URL_B, URL_B trong response_B có thể được thay thế bằng URL_A hoặc URL_A trong response_A và URL_B trong response_B có thể đều được thay thế bằng URL_C trước khi so sánh.

Theo một số phương án thực hiện, để đáp lại việc xác định rằng không cần xác minh đăng nhập thứ cấp để kết nối với mạng không dây, việc xác định được thực hiện mà sự kết nối với mạng không dây không phải là kết nối bảo mật. Thông báo cảnh báo có thể được hiển thị trên thiết bị di động để nhắc người dùng về rủi ro bảo mật tiềm tàng của việc kết nối với mạng không dây. Theo một số phương án thực hiện, kết nối với mạng không dây được chặn tự động bởi, ví dụ, ứng dụng bảo mật trên thiết bị di động để đáp lại việc xác định rằng việc kết nối với mạng không dây không phải là kết nối bảo mật.

Theo một số phương án thực hiện, để đáp lại việc xác định rằng việc xác minh đăng nhập thứ cấp là cần thiết để kết nối với mạng không dây, việc xác định được thực hiện mà sự kết nối với mạng không dây là kết nối bảo mật. Trong trường hợp này, người dùng có thể nhập tên người dùng, mật khẩu hoặc kết hợp của cả hai trên thiết bị di động để kết nối với mạng không dây. Nếu thiết bị di động có tên người dùng được lưu trữ, mật khẩu được lưu trữ hoặc kết hợp của cả hai đối với mạng không dây, thiết bị di động này có thể cung cấp tên người dùng, mật khẩu hoặc kết hợp của cả hai một cách tự động để kết nối với mạng không dây. Do việc kết nối với mạng không dây được xác định là kết nối bảo mật, nên không có cảnh báo nguy cơ bảo mật về kết nối được hiển thị trên thiết bị di động và kết nối với mạng không dây không được chặn bởi, ví dụ ứng dụng bảo mật trên thiết bị di động. Sau bước 515, phương pháp 500 dừng lại.

Người dùng có thể sử dụng phần mềm ứng dụng được cài đặt trên thiết bị di động để kết nối với mạng không dây qua, ví dụ trạm phát Wi-Fi. Thông thường, các trạm phát Wi-Fi không bảo mật không có mật khẩu đăng nhập. Tuy nhiên, một số trạm phát Wi-Fi bảo mật cũng không có các mật khẩu đăng nhập trong khi thực hiện quy trình xác minh đăng nhập thứ cấp. Kết quả là, thiết bị di động không thể phân biệt trạm phát Wi-Fi không bảo mật mà không có mật khẩu đăng nhập với trạm phát Wi-Fi bảo mật có xác minh đăng nhập thứ cấp. Ứng dụng bảo mật trên thiết bị di động sẽ xử lý

trạm phát Wi-Fi bảo mật có xác minh đăng nhập thứ cấp theo cùng cách với trạm phát Wi-Fi không bảo mật mà không có mật khẩu đăng nhập, do vậy dẫn đến sự trải nghiệm của người dùng kém khi sử dụng ứng dụng bảo mật này. Đối tượng được mô tả trong bản mô tả này có thể được sử dụng để phân biệt trạm phát Wi-Fi không bảo mật mà không có mật khẩu đăng nhập với trạm phát Wi-Fi bảo mật có xác minh đăng nhập thứ cấp. Ví dụ, sau khi xác định rằng trạm phát Wi-Fi không có mật khẩu đăng nhập, bước xác định khác được thực hiện để xem liệu trạm phát Wi-Fi không có mật khẩu đăng nhập có thực hiện quy trình xác minh đăng nhập thứ cấp hay không. Kết quả là, trạm phát Wi-Fi, không có mật khẩu đăng nhập và có xác minh đăng nhập thứ cấp, có thể được nhận dạng một cách chính xác là trạm phát Wi-Fi bảo mật. Theo đó, nguy cơ bảo mật mạng chính xác của kết nối Wi-Fi có thể được cung cấp cho người dùng, nhờ đó làm giảm mức độ đánh giá sai của kết nối Wi-Fi và sự phiền phức cho người dùng.

Các phương án và hoạt động được mô tả trong bản mô tả này có thể được thực hiện trong mạch điện tử kỹ thuật số hoặc phần mềm, phần sụn hoặc phần cứng máy tính, bao gồm các kết cấu được bộc lộ trong bản mô tả này hoặc trong các kết hợp của một hoặc nhiều trong số chúng. Các hoạt động có thể được thực hiện khi các hoạt động được thực hiện bởi thiết bị xử lý dữ liệu đối với dữ liệu được lưu trữ trên một hoặc nhiều thiết bị lưu trữ đọc được bằng máy tính hoặc được nhận từ các nguồn khác. Thiết bị xử lý dữ liệu, máy tính hoặc thiết bị điện toán có thể bao gồm thiết bị, các phương tiện và các máy để xử lý dữ liệu, bao gồm bằng cách lấy ví dụ, bộ xử lý lập trình được, máy tính, hệ thống trên một chip hoặc một số phức hợp hoặc các kết hợp của các thành phần nêu trên. Thiết bị có thể bao gồm mạch logic chuyên dụng, ví dụ, bộ xử lý trung tâm (CPU), mảng cổng lập trình được dạng trường (FPGA) hoặc mạch tích hợp chuyên dụng (ASIC). Thiết bị cũng có thể bao gồm mã tạo ra môi trường thực thi chương trình máy tính được đề cập, ví dụ mã cấu thành phần sụn xử lý, chồng giao thức, hệ thống quản lý cơ sở dữ liệu, hệ điều hành (ví dụ, một hệ điều hành hoặc kết hợp của các hệ điều hành), môi trường thời gian chạy đa nền tảng, máy ảo hoặc kết hợp của một hoặc nhiều trong số chúng. Thiết bị và môi trường thực thi có thể nhận ra các hạ tầng mô hình điện toán khác nhau như các dịch vụ web, các hạ tầng điện toán phân toán và điện toán lưới.

Chương trình máy tính (còn được biết là, ví dụ như chương trình, phần mềm, ứng dụng phần mềm, môđun phần mềm, đơn vị phần mềm, tập lệnh hoặc mã) có thể được viết dưới dạng ngôn ngữ lập trình bất kỳ, bao gồm các ngôn ngữ biên dịch hoặc thông dịch, các ngôn ngữ khai báo hoặc thủ tục và có thể được triển khai dưới dạng bất kỳ, bao gồm dưới dạng chương trình độc lập hoặc dưới dạng môđun, thành phần, chương trình con, đối tượng hoặc đơn vị khác thích hợp để sử dụng trong môi trường điện toán. Chương trình có thể được lưu trữ trong một phần của tệp tin chứa các chương trình hoặc dữ liệu khác (ví dụ, một hoặc nhiều tập lệnh được lưu trữ trong tài liệu ngôn ngữ đánh dấu), trong một tệp tin được dành riêng cho chương trình được đề cập hoặc trong nhiều tệp tin kết hợp (ví dụ, các tệp tin lưu trữ một hoặc nhiều môđun, các chương trình con hoặc các phần mã). Chương trình máy tính có thể được thực thi trên một máy tính hoặc trên nhiều máy tính nằm ở một vị trí hoặc được phân tán tại nhiều vị trí và được kết nối bởi mạng truyền thông.

Các bộ xử lý để thực thi chương trình máy tính bao gồm, bằng cách lấy ví dụ, cả các bộ vi xử lý chung và chuyên dụng và một hoặc nhiều bộ xử lý bất kỳ của loại máy tính kỹ thuật số bất kỳ. Nói chung, bộ xử lý sẽ nhận các lệnh và dữ liệu từ bộ nhớ chỉ đọc hoặc bộ nhớ truy cập ngẫu nhiên hoặc cả hai. Các thành phần thiết yếu của máy tính là bộ xử lý để thực hiện các hoạt động theo các lệnh và một hoặc nhiều thiết bị bộ nhớ để lưu trữ các lệnh và dữ liệu. Nói chung, máy tính cũng sẽ bao gồm hoặc được ghép nối theo cách vận hành để nhận dữ liệu từ hoặc truyền dữ liệu đến, hoặc cả hai, một hoặc nhiều thiết bị lưu trữ khối để lưu trữ dữ liệu. Máy tính có thể được nhúng trong trong thiết bị khác, ví dụ, thiết bị di động, thiết bị hỗ trợ kỹ thuật số cá nhân (PDA), bàn điều khiển trò chơi, bộ thu hệ thống định vị toàn cầu (GPS) hoặc thiết bị lưu trữ di động. Các thiết bị thích hợp để lưu trữ các lệnh chương trình máy tính và dữ liệu bao gồm bộ nhớ không khả biến, vật ghi và các thiết bị bộ nhớ, bao gồm, bằng cách lấy ví dụ, các thiết bị bộ nhớ bán dẫn, đĩa từ và đĩa quang-từ. Bộ xử lý và bộ nhớ có thể được bổ sung bởi hoặc được kết hợp vào mạch logic chuyên dụng.

Các thiết bị di động có thể bao gồm thiết bị cầm tay, thiết bị người dùng (UE), điện thoại di động (ví dụ, điện thoại thông minh), máy tính bảng, thiết bị đeo được (ví dụ, đồng hồ thông minh và kính mắt thông minh), thiết bị được cấy trong cơ thể người (ví dụ, bộ cảm biến sinh học, linh kiện cấy ốc tai) hoặc các loại thiết bị di động khác. Các thiết bị di động có thể truyền thông không dây (ví dụ, sử dụng các tín hiệu tần số

vô tuyến (RF)) với các mạng truyền thông khác nhau (được mô tả dưới đây). Các thiết bị di động có thể bao gồm các bộ cảm biến để xác định các đặc tính của môi trường hiện tại của thiết bị di động. Các bộ cảm biến có thể bao gồm các camera, micro, bộ cảm biến tiệm cận, bộ cảm biến GPS, bộ cảm biến chuyển động, gia tốc kế, bộ cảm biến ánh sáng xung quanh, bộ cảm biến độ ẩm, con quay hồi chuyển, la bàn, các bộ đo khí áp, bộ cảm biến dấu vân tay, hệ thống nhận dạng khuôn mặt, bộ cảm biến RF (ví dụ, Wi-Fi và thiết bị vô tuyến mạng tế bào), bộ cảm biến nhiệt hoặc các loại cảm biến khác. Ví dụ, camera có thể bao gồm camera hướng về phía trước và phía sau có các ống kính di động và cố định, đèn chớp, bộ cảm biến hình ảnh và bộ xử lý hình ảnh. Camera có thể là camera triệu điểm ảnh, có khả năng chụp các chi tiết để nhận dạng khuôn mặt và/hoặc nhận dạng mống mắt. Camera cùng với bộ xử lý dữ liệu và thông tin xác minh được lưu trữ trong bộ nhớ hoặc được truy cập từ xa có thể tạo thành hệ thống nhận dạng khuôn mặt. Hệ thống nhận dạng khuôn mặt hoặc một hoặc nhiều bộ cảm biến, ví dụ, các micro, bộ cảm biến chuyển động, gia tốc kế, bộ cảm biến GPS hoặc bộ cảm biến RF, có thể được sử dụng để xác thực người dùng.

Để tạo sự tương tác với người dùng, các phương án có thể được thực hiện trên máy tính có thiết bị hiển thị và thiết bị đầu vào, ví dụ màn hiển thị tinh thể lỏng (LCD) hoặc điốt phát quang hữu cơ (OLED)/màn hiển thị thực tế ảo (VR) /thực tế tăng cường (AR) để hiển thị thông tin đến người dùng và màn hình chạm, bàn phím và thiết bị trở mà người dùng có thể cung cấp đầu vào cho máy tính. Các loại thiết bị khác có thể được sử dụng để cung cấp tương tác với người dùng; ví dụ, phản hồi được cung cấp đến người dùng có thể là ở dạng bất kỳ của phản hồi cảm giác, ví dụ phản hồi trực quan, phản hồi âm thanh hoặc phản hồi xúc giác; và đầu vào từ người dùng có thể được nhận ở dạng bất kỳ, bao gồm đầu vào âm thanh, giọng nói hoặc xúc giác. Ngoài ra, máy tính có thể tương tác với người dùng bằng cách gửi các tài liệu đến và nhận các tài liệu từ thiết bị được sử dụng bởi người dùng; ví dụ bằng cách gửi các trang web đến trình duyệt web trên thiết bị máy khách của người dùng để đáp lại các yêu cầu được nhận từ trình duyệt web.

Các phương án có thể được thực hiện bằng cách sử dụng các thiết bị điện toán được kết nối bởi dạng bất kỳ hoặc phương tiện truyền thông dữ liệu có dây hoặc không dây (hoặc kết hợp của chúng), ví dụ mạng truyền thông. Các ví dụ của các thiết bị được kết nối là máy khách và máy chủ, thường là cách xa nhau, thường tương tác

qua mạng truyền thông. Máy khách, ví dụ thiết bị di động, có thể thực hiện chính các giao dịch với máy chủ hoặc qua máy chủ, ví dụ thực hiện việc mua, bán, thanh toán, trao, gửi hoặc các giao dịch vay hoặc ủy quyền. Các giao dịch này có thể theo thời gian thực như là hoạt động và phản hồi là gần nhau về mặt thời gian; ví dụ người dùng cảm nhận hành động và phản hồi là xảy ra gần như đồng thời, sự chênh lệch về thời gian đối với phản hồi sau hoạt động của người dùng là nhỏ hơn 1 mili giây (ms) hoặc là nhỏ hơn 1 giây (s) hoặc phản hồi không có độ trễ nội hàm khi tính đến các giới hạn xử lý của hệ thống.

Các ví dụ của các mạng truyền thông bao gồm mạng cục bộ (LAN), mạng truy cập vô tuyến (RAN), mạng đô thị (MAN) và mạng diện rộng (WAN). Mạng truyền thông có thể bao gồm tất cả hoặc một phần của Internet, mạng truyền thông khác hoặc kết hợp của các mạng truyền thông. Thông tin có thể được truyền trên mạng truyền thông theo các giao thức và tiêu chuẩn khác nhau, bao gồm tiến hóa dài hạn (LTE), 5G, IEEE 802, giao thức Internet (IP) hoặc các giao thức khác hoặc các kết hợp của các giao thức. Mạng truyền thông có thể truyền dữ liệu giọng nói, dữ liệu video, dữ liệu sinh trắc học hoặc dữ liệu xác thực hoặc thông tin khác giữa các thiết bị điện toán được kết nối.

Các dấu hiệu được mô tả bởi các phương án thực hiện riêng rẽ có thể được thực hiện kết hợp trong một phương án thực hiện, mặc dù các dấu hiệu được mô tả bởi một phương án thực hiện có thể được thực hiện trong nhiều phương án thực hiện, một cách riêng rẽ hoặc theo sự kết hợp con phù hợp bất kỳ. Các hoạt động được mô tả và được bảo hộ theo thứ tự cụ thể không được hiểu là yêu cầu thứ tự cụ thể này, cũng như không phải tất cả các hoạt động được minh họa phải được thực hiện (một số hoạt động có thể là tùy ý). Khi thích hợp, xử lý đa nhiệm hoặc song song (hoặc kết hợp của xử lý xử lý đa nhiệm và song song) có thể được thực hiện.

YÊU CẦU BẢO HỘ

1. Phương pháp phát hiện kiểu mạng không dây được thực hiện bởi thiết bị điện tử, phương pháp này bao gồm các bước:

xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để truy cập Internet qua mạng không dây hay không dựa vào ít nhất một địa chỉ mạng được chỉ định (202);

truy cập địa chỉ mạng chỉ định (204) để đáp lại bước xác định rằng không cần mật khẩu;

xác định xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không bằng cách xác định xem liệu địa chỉ mạng chỉ định có thể được truy cập thành công hay không (206);

xác định rằng mạng không dây được kết nối hiện tại là mạng không bảo mật nếu mạng không dây được kết nối hiện tại này không cần mật khẩu và không cần mật khẩu thứ cấp; và

cung cấp cảnh báo rủi ro bảo mật đến người dùng thiết bị điện tử hoặc tự động chặn truy cập bởi thiết bị điện tử với mạng không dây được kết nối hiện tại, nếu mạng không dây được kết nối hiện tại này là mạng không bảo mật.

2. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước tự động chặn truy cập bởi thiết bị điện tử với mạng không dây được kết nối hiện tại, nếu mạng không dây được kết nối hiện tại này là mạng không bảo mật.

3. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước cung cấp cảnh báo rủi ro bảo mật đến người dùng thiết bị điện tử.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó bước xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không bao gồm các bước:

gọi giao diện quản lý mật khẩu mạng không dây được cung cấp bởi hệ điều hành;

thu kết quả gọi; và

xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để kết nối hay không dựa vào kết quả gọi.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó địa chỉ mạng được chỉ định bao gồm địa chỉ mạng của API được định nghĩa bởi người dùng cho doanh nghiệp và API được định nghĩa bởi người dùng này được sử dụng để trả về thông tin nhận dạng cụ thể khi API được truy cập.

6. Phương pháp theo điểm 5, trong đó bước xác định xem liệu địa chỉ mạng được chỉ định có được truy cập thành công hay không bao gồm bước: thu kết quả truy cập của việc truy cập địa chỉ mạng của API được định nghĩa bởi người dùng; phương pháp này còn bao gồm bước:

xác định xem liệu địa chỉ mạng của API được định nghĩa bởi người dùng có thể được truy cập thành công hay không dựa vào việc liệu kết quả truy cập có bao gồm thông tin nhận dạng cụ thể hay không.

7. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó địa chỉ mạng chỉ định bao gồm các địa chỉ mạng của ít nhất hai trang web khác nhau.

8. Phương pháp theo điểm 7, trong đó bước xác định xem liệu địa chỉ mạng chỉ định có thể được truy cập thành công hay không bao gồm bước:

thu dữ liệu trang web được trả về sau khi địa chỉ mạng của mỗi trong số các trang web được truy cập và xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không bằng cách so sánh dữ liệu trang web của các trang web, để xác định xem liệu địa chỉ mạng chỉ định của trang web có thể được truy cập thành công hay không.

9. Phương pháp theo điểm 8, trong đó dữ liệu trang web của trang web bao gồm địa chỉ mạng của trang web.

10. Phương pháp theo điểm 8, trong đó bước xác định xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không bằng cách so sánh dữ liệu trang web của các trang web, bao gồm các bước:

cập nhật dữ liệu trang web của mỗi trong số các trang web, trong đó bước cập nhật này bao gồm bước xóa địa chỉ mạng được bao gồm trong dữ liệu trang web của

mỗi trong số các trang web hoặc thay thế địa chỉ mạng được bao gồm trong dữ liệu trang web của mỗi trong số các trang web bằng dữ liệu nhận dạng thống nhất; và

so sánh dữ liệu trang web được cập nhật của các trang web để xác định xem liệu dữ liệu trang web có giống nhau hay không và xác định dựa vào kết quả so sánh, xem liệu mỗi trang web được truy cập có chuyển đến trang xác minh đăng nhập thứ cấp hay không.

11. Thiết bị điện tử bao gồm:

bộ xử lý; và

bộ nhớ được tạo cấu hình để lưu trữ lệnh mà có thể được thực thi bởi bộ xử lý, trong đó bộ xử lý này được tạo cấu hình để:

xác định xem liệu mạng không dây được kết nối hiện tại có cần mật khẩu để truy cập dịch vụ qua mạng không dây hay không dựa vào địa chỉ mạng chỉ định (202);

sau khi xác định rằng không cần mật khẩu, truy cập ít nhất một địa chỉ mạng chỉ định (204);

xác định xem liệu mạng không dây được kết nối hiện tại có cần xác minh đăng nhập thứ cấp hay không bằng cách xác định xem liệu địa chỉ mạng chỉ định có thể được truy cập thành công hay không (206);

xác định rằng mạng không dây được kết nối hiện tại là mạng không bảo mật nếu mạng không dây được kết nối hiện tại này không cần mật khẩu và không cần mật khẩu thứ cấp; và

cung cấp cảnh báo rủi ro bảo mật đến người dùng thiết bị điện tử hoặc tự động chặn truy cập bởi thiết bị điện tử với mạng không dây được kết nối hiện tại, nếu mạng không dây được kết nối hiện tại này là mạng không bảo mật.

12. Thiết bị theo điểm 11, trong đó bộ nhớ bao gồm thiết bị phát hiện kiểu mạng không dây được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 10.

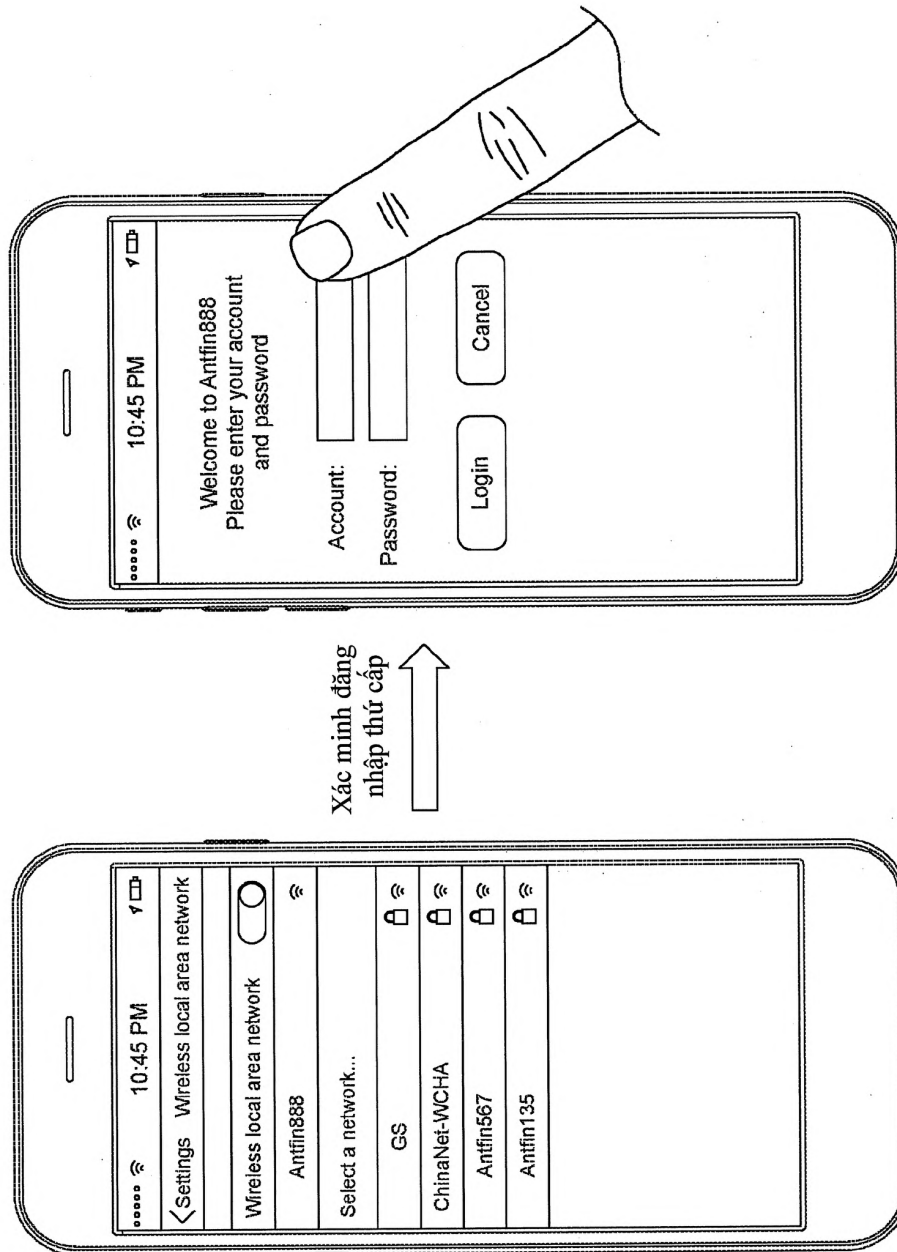
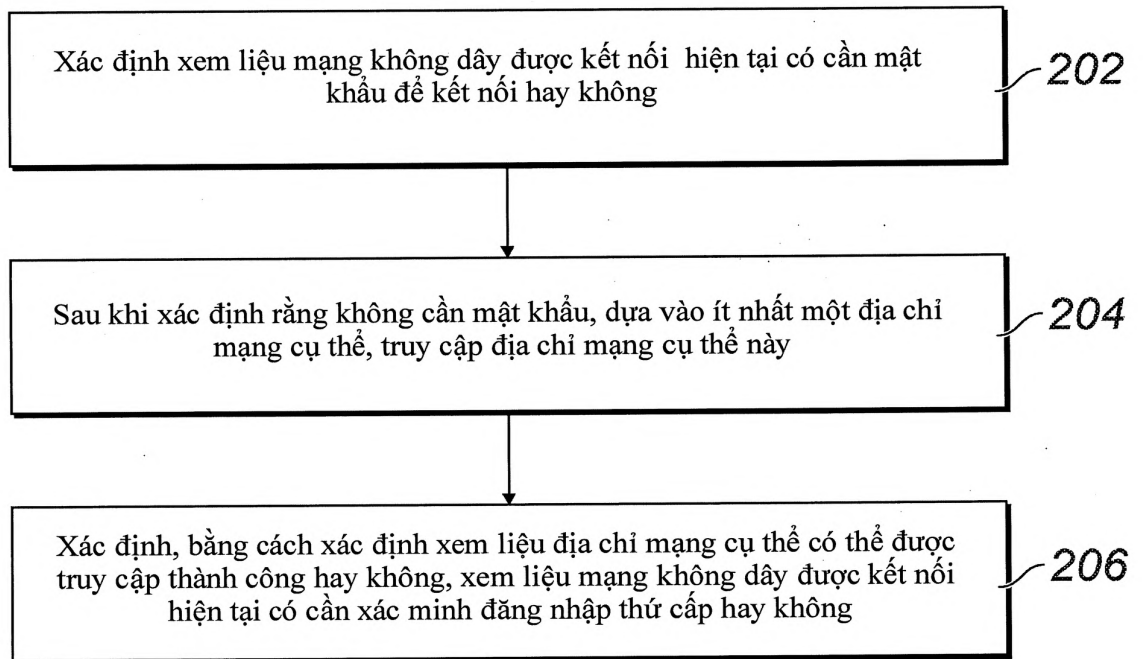
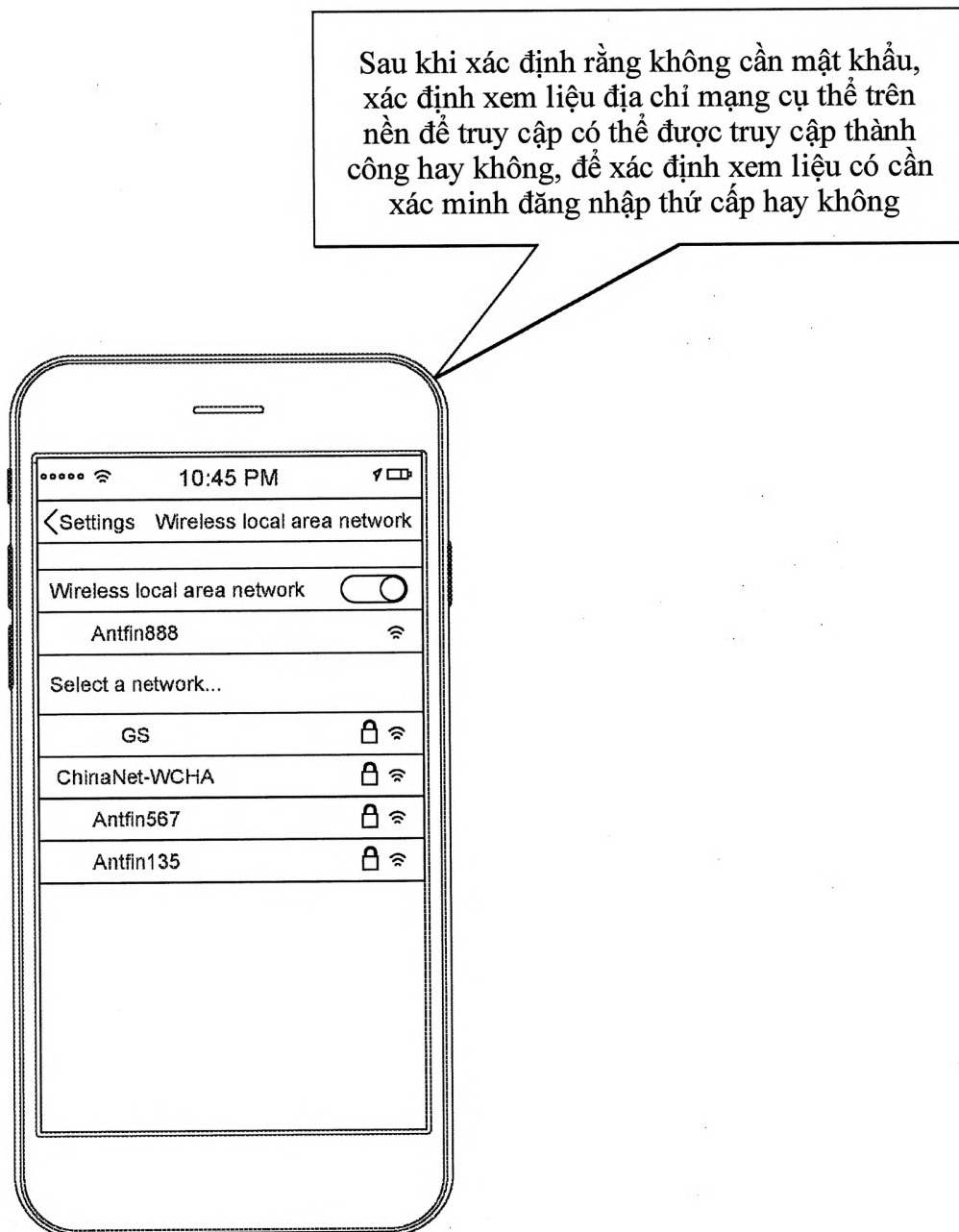


FIG. 1

**FIG. 2A**

**FIG. 2B**

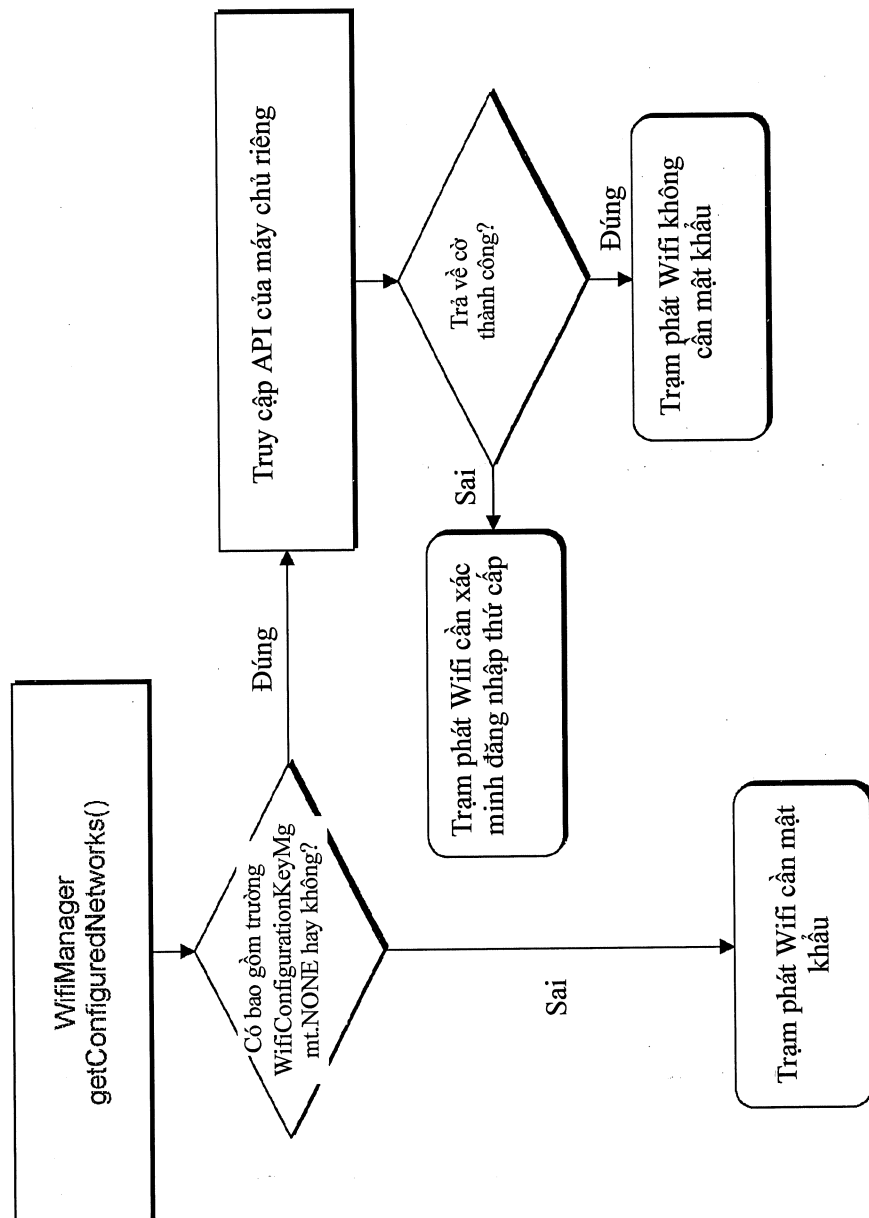


FIG. 2C

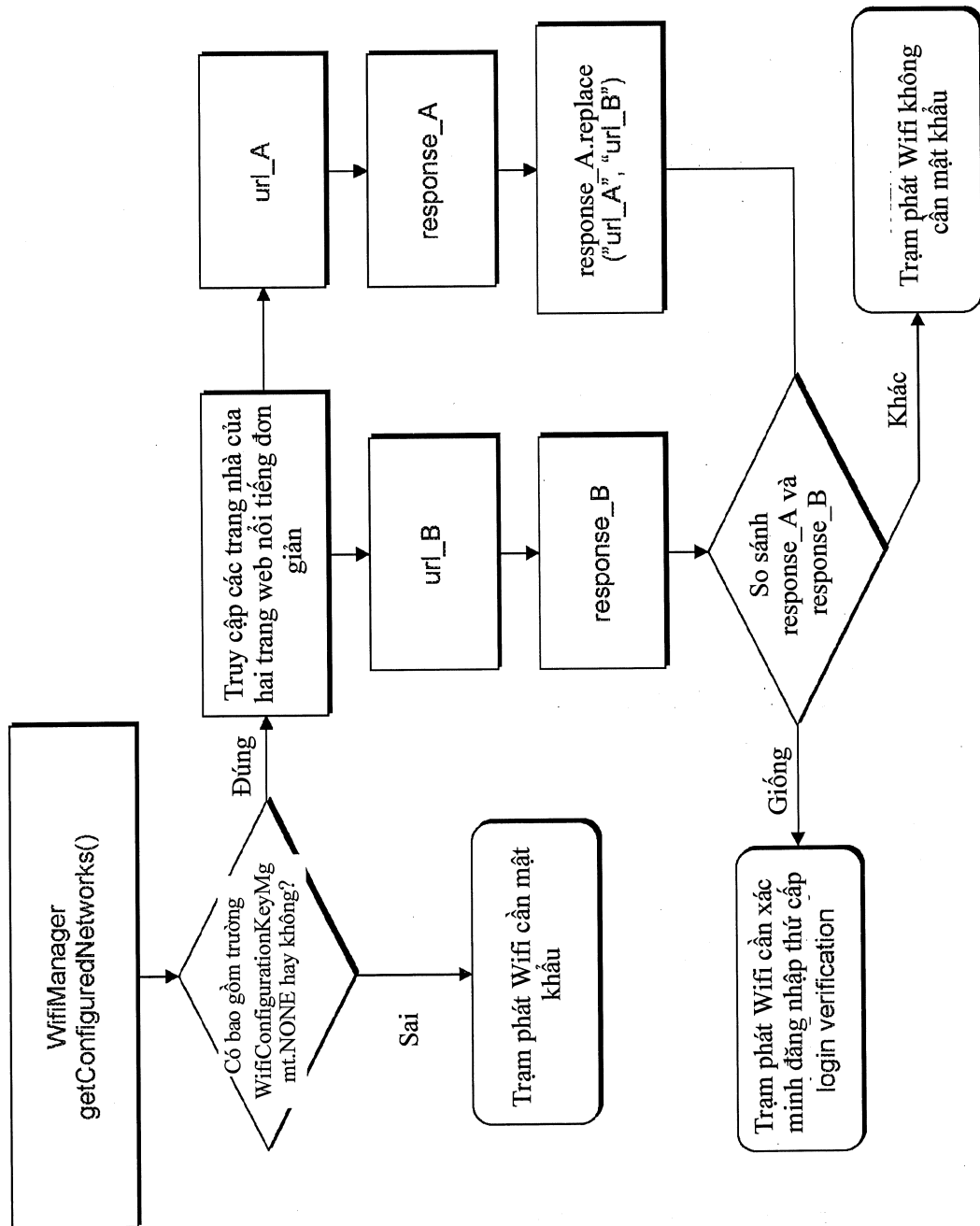


FIG. 2D

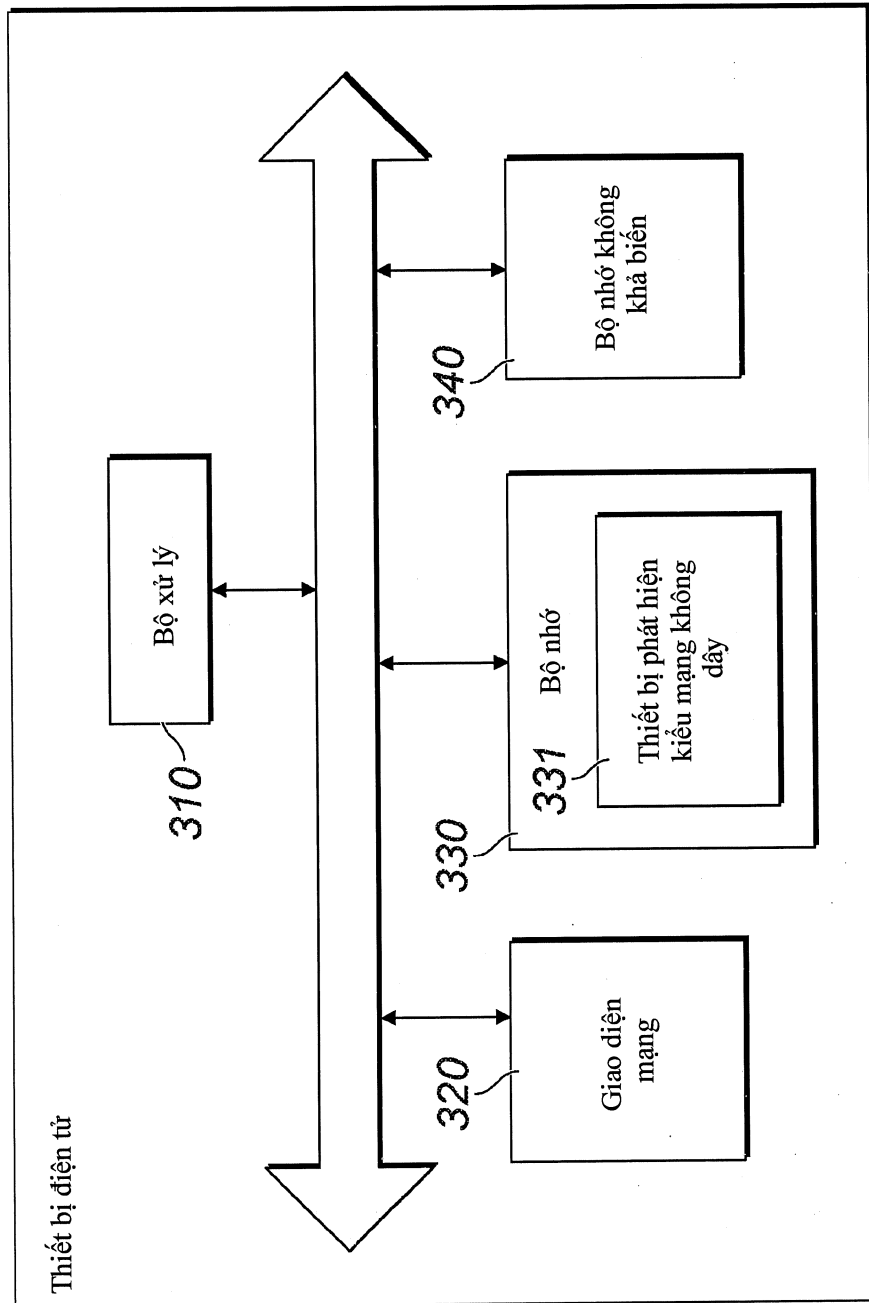


FIG. 3

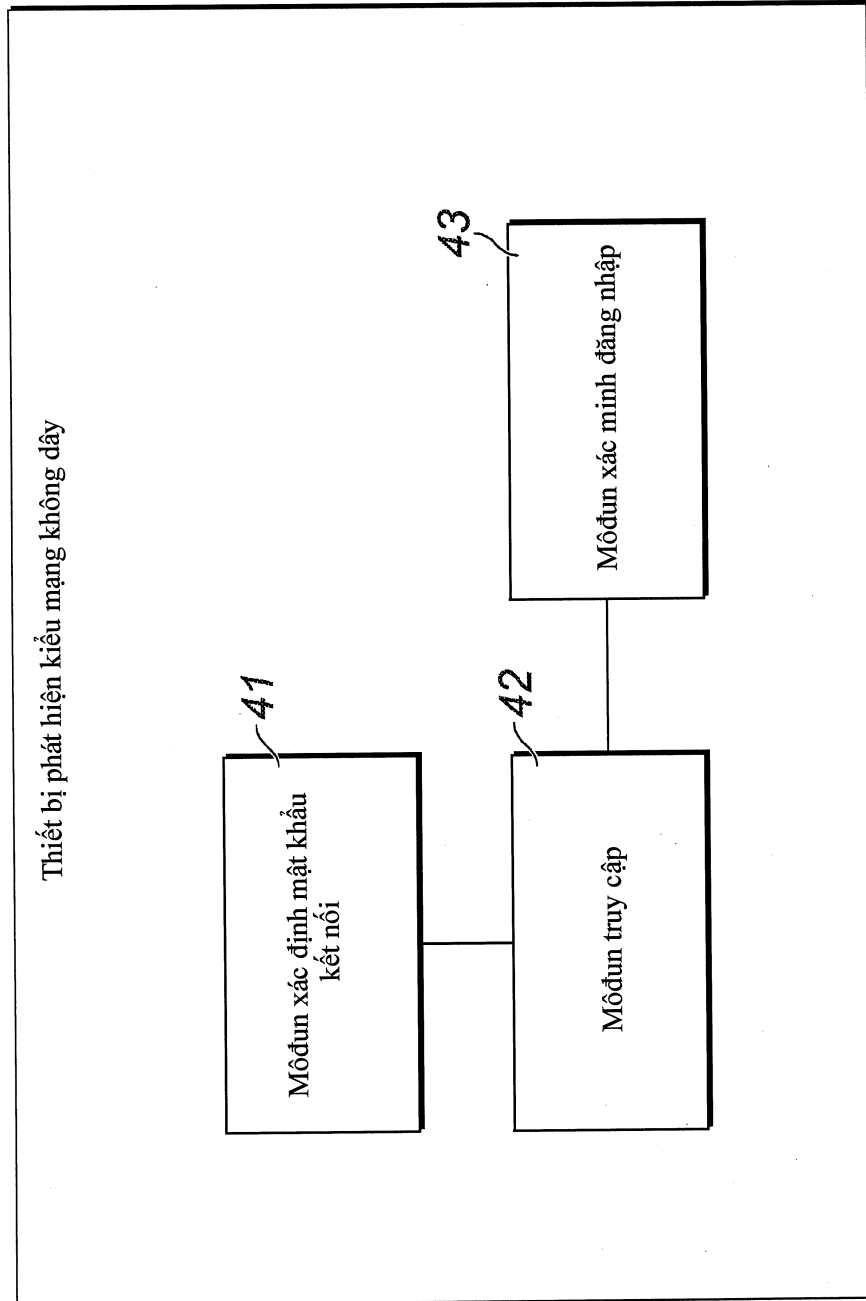
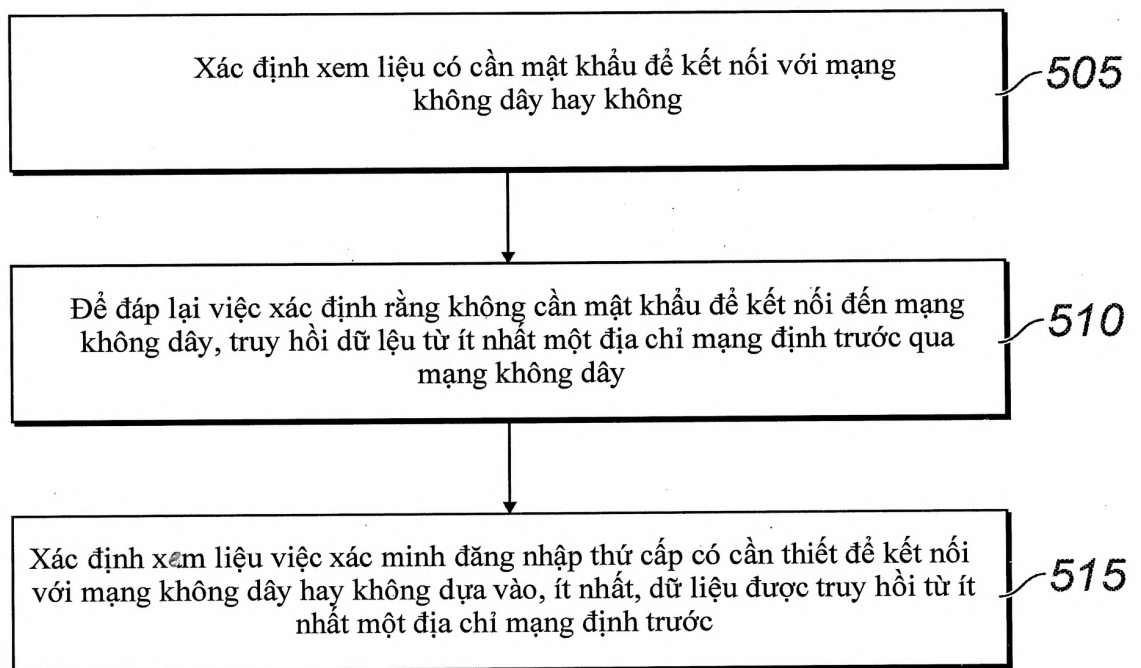


FIG. 4

**FIG. 5**