(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) **1-0030652**

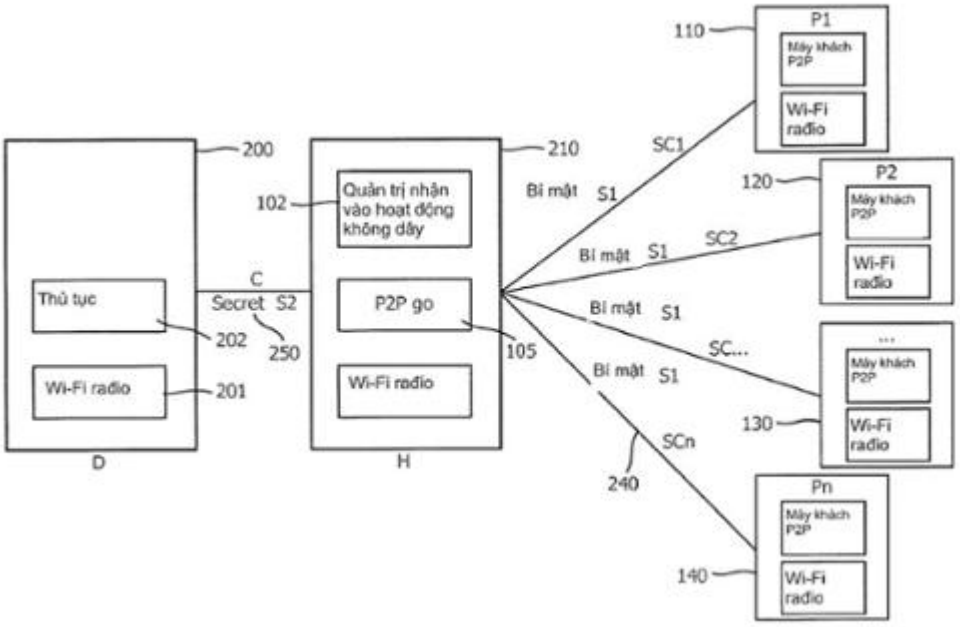
(51)[7] **H04W 12/04**; H04L 29/06

(13) **B**

(21) 1-2015-01063 (22) 29/08/2013
(86) PCT/EP2013/067868 29/08/2013 (87) WO/2014/033199 06/03/2014
(30) 61/695,022 30/08/2012 US; 12182285.2 30/08/2012 EP
(45) 25/01/2022 406 (43) 26/10/2015 331A
(73) Koninklijke Philips N.V. (NL)
High Tech Campus 5 NL-5656 AE Eindhoven Netherlands
(72) DEES, Walter (NL); BERNSEN, Johannes Arnoldus Cornelis (NL).
(74) Công ty TNHH T&T INVENMARK Sở hữu trí tuệ Quốc tế (T&T INVENMARK CO., LTD.)

(54) HỆ THỐNG, PHƯƠNG PHÁP VÀ THIẾT BỊ TRUYỀN THÔNG KHÔNG DÂY

(57) Sáng chế đề cập đến hệ thống truyền thông không dây bao gồm nhóm thiết bị không dây (110, 120, 130, 140) bao gồm ít nhất một thiết bị máy chủ không dây (100) được kết nối bảo mật dựa trên dữ liệu bí mật thứ nhất (240) được chia sẻ bởi nhóm. Kết nối bảo mật thứ hai được thiết lập giữa thiết bị mang được không dây (200) và thiết bị máy chủ không dây dựa trên dữ liệu bí mật thứ hai (250). Ít nhất một trong số thiết bị không dây nhận lệnh áp dụng dữ liệu bí mật thứ ba cho việc thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được không dây (200). Ngoài ra thiết bị mang được không dây nhận lệnh thông qua kết nối bảo mật thứ hai để áp dụng dữ liệu bí mật thứ ba cho việc thiết lập kết nối bảo mật trực tiếp với thiết bị không dây dựa trên dữ liệu bí mật thứ ba. Cuối cùng, kết nối bảo mật không dây trực tiếp tương ứng được thiết lập giữa thiết bị thứ hai và thiết bị không dây tương ứng dựa trên dữ liệu bí mật thứ ba. Độ trễ trong hoạt động nhận vào hoạt động không dây bảo mật được giảm bớt.


200
Thủ tục
202
Wi-Fi radio
201
D
C
Secret S2
250
102
Quản trị nhận vào hoạt động không dây
P2P go
105
Wi-Fi radio
H
210
Bí mật S1
SC1
110
P1
Máy khách P2P
Wi-Fi radio
Bí mật S1
SC2
120
P2
Máy khách P2P
Wi-Fi radio
Bí mật S1
SC...
...
Máy khách P2P
Wi-Fi radio
130
Bí mật S1
SCn
240
Pn
Máy khách P2P
Wi-Fi radio
140

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống truyền thông không dây bao gồm nhóm thiết bị không dây và thiết bị mang được, mỗi thiết bị bao gồm bộ thu phát rađio không dây để trao đổi dữ liệu với thiết bị khác, thiết bị không dây thứ nhất của nhóm cung cấp chức năng máy chủ thứ nhất và thiết bị không dây thứ hai của nhóm cung cấp chức năng máy chủ thứ hai, thiết bị không dây thứ nhất và thiết bị không dây thứ hai là thiết bị không dây giống nhau hoặc là thiết bị không dây khác nhau, nhóm thiết bị không dây chia sẻ dữ liệu bí mật thứ nhất và được tạo cấu hình cho truyền thông không dây với thiết bị không dây thứ nhất cung cấp chức năng máy chủ thứ nhất thông qua kết nối bảo mật tương ứng thứ nhất dựa trên dữ liệu bí mật thứ nhất. Sáng chế còn đề cập đến thiết bị mang được, thiết bị máy chủ, thiết bị không dây, phương pháp và sản phẩm máy tính để sử dụng trong hệ thống truyền thông không dây. Sáng chế đề cập đến lĩnh vực truyền thông không dây bảo mật, ví dụ như thông qua Wi-Fi, và cụ thể hơn đến việc thiết lập bảo mật cho hệ thống không dây.

Tình trạng kỹ thuật của sáng chế

Trong truyền thông không dây, như Wi-Fi được biết đến từ IEEE 802.11, thiết bị cần phải được ghép cặp để thiết lập kết nối bảo mật, ví dụ như được mô tả trong tài liệu "Wi-Fi Protected Access (WPA), Enhanced Security Implementation Based on IEEE P802.1li, Phiên bản 3.1, tháng tám, năm 2004, của Liên minh Wi-Fi" có sẵn tại www.wi-fi.org. Mặc dù sáng chế được mô tả bằng cách viện dẫn tới hệ thống Wi-Fi nhưng cần lưu ý rằng sáng chế có thể cũng được áp dụng trong các hệ thống truyền thông không dây khác, chẳng hạn như, Bluetooth (xem ví dụ BLUETOOTH SPECIFICATION, phiên bản Core Package 2.1 + EDR, ban hành: 26 tháng bảy 2007).

Các kết nối Wi-Fi được bảo vệ nhằm mục đích bảo mật và để đảm bảo tính toàn vẹn nhờ phương tiện mã hóa, sử dụng các công nghệ như WPA2. Tính bảo mật trong WPA2 có thể dựa trên hai hệ thống. Hệ thống thứ nhất là PSK (Pre-Shared Key mode-chế độ khóa dung chung trước, còn được gọi là chế độ cá nhân) và được thiết kế cho

mạng gia đình và văn phòng nhỏ. Hệ thống thứ hai dựa trên việc sử dụng máy chủ xác thực 802. IX và được thiết kế cho các mạng doanh nghiệp.

Trong chế độ PSK, tất cả thiết bị giao tiếp với nhau chia sẻ khóa 256 bit, còn được gọi là 'Passphrase'. Cấu hình Wi-Fi đơn giản (thiết lập Wi-Fi được bảo vệ), được biết đến từ tài liệu "Wi-Fi cấu hình đơn giản, đặc tả kỹ thuật, phiên bản 2.0.2, 2011", cũng từ Liên minh Wi-Fi, là tiêu chuẩn cho phép thiết bị thứ nhất mà biết Passphrase, ví dụ như điểm truy cập mạng LAN không dây, gửi nó đến thiết bị thứ hai theo cách bảo mật, mà người dùng không cần phải nhập vào mật khẩu trên thiết bị thứ hai. Thay vào đó, người dùng có thể, ví dụ, nhấn nút trên cả hai thiết bị trong một thời gian giới hạn, hoặc nhập mã PIN 8 chữ số được liệt kê trên thiết bị thứ nhất trong thiết bị thứ hai, để nhận được mật khẩu. Điều này thường liên quan đến hành động của người dùng, tức là, hoạt động được gọi hoạt động ghép cặp người dùng.

US2010/0153727 mô tả việc bảo mật tăng cường cho truyền thông liên kết trực tiếp giữa nhiều thiết bị không dây, mà trao đổi các nonce (số nhị phân được sử dụng một lần khi mã hóa) được sử dụng để tạo ra nonce chung. Phần tử thông tin nhận dạng nhóm được tạo ra từ ít nhất 15 nonce chung và được chuyển tiếp đến máy chủ xác thực. Máy chủ xác thực tạo ra khóa chính của liên kết trực tiếp của nhóm từ phần tử thông tin nhận dạng nhóm để so khớp thiết bị như là một phần của nhóm thỏa thuận của khóa. Các khóa nhóm cũng được tạo ra dựa trên nonce chung. Vì vậy, nhóm bảo mật của thiết bị cho truyền thông liên kết trực tiếp được tạo ra.

Trong cơ sở hạ tầng Wi-Fi, AP (Access Point – điểm truy cập), hay đúng hơn là bộ nhận đăng ký, lưu trữ và quản lý bằng chứng tin cậy cho mạng mà nó chịu trách nhiệm. Thiết bị Wi-Fi mà muốn truy cập vào mạng cơ sở hạ tầng Wi-Fi của AP cần thu được bằng chứng tin cậy trong hoạt động ghép cặp với AP này. Sau khi kết nối bảo mật với AP được thiết lập, thiết bị Wi-Fi có thể giao tiếp với thiết bị Wi-Fi khác gắn với AP này. Cơ sở hạ tầng truyền thống có bất lợi là kết nối gián tiếp, bởi vì tất cả truyền thông cần phải đi qua điểm truy cập. Tuy nhiên, trong nhiều trường hợp, nó có lợi (ví dụ, giảm độ trễ, cải thiện tốc độ kết nối) mà thiết bị này sẽ có thể thiết lập liên kết trực tiếp với nhau mà không cần phải chuyển tiếp lưu lượng truy cập thông qua điểm truy cập. Hai công nghệ Wi-Fi Direct và thiết lập liên kết trực tiếp được tạo đường truyền (TDLS) đã được tạo ra để có thể thiết lập liên kết Wi-Fi trực tiếp loại này giữa các thiết bị.

Wi-Fi Direct (Wi-Fi ngang hàng), được biết đến từ "Wi-Fi Wi-Fi Peer-to-Peer (P2P) đặc tả kỹ thuật, phiên bản 1.1, 2010", cũng từ liên minh Wi-Fi là tiêu chuẩn cho phép thiết bị Wi-Fi kết nối với nhau và không cần điểm truy cập không dây. Wi-Fi Direct đóng vai trò quan trọng để kết nối thiết bị không dây độc lập và thiết bị ngoại vi, chẳng hạn như, thiết bị hiển thị/thiết bị ngoại vi hỗ trợ hiển thị Wi-Fi, và thiết bị I/O (vào/ra)/thiết bị ngoại vi hỗ trợ Wi-Fi Serial Bus (ví dụ như chuột không dây, bàn phím, máy in, USB). Do đó, công nghệ quan trọng cho nền không dây, là công nghệ cho phép thiết bị mang được kết nối với nhiều thiết bị ngoại vi không dây. Trong Wi-Fi Direct, bước ghép cặp người dùng thường cần phải được thực hiện cho mỗi kết nối Wi-Fi Direct mới được tạo ra. Khi hai thiết bị Wi-Fi muốn giao tiếp, một trong số chúng sẽ trở thành cái gọi là chủ sở hữu nhóm (GO). Thiết bị kia sẽ đóng vai trò thiết bị khách. Chúng cùng nhau tạo thành cái gọi là nhóm P2P. Một GO có nhiều điểm tương đồng với AP. Nó có thể, ví dụ, cho phép thiết bị khác tham gia vào nhóm P2P, và cung cấp khả năng phân phối lưu lượng giữa các thiết bị khác nhau trong nhóm P2P. Tuy nhiên, như đã đề cập trên đây, có lợi nếu các thiết bị có thể giao tiếp trực tiếp với nhau mà không cần phải chuyển tiếp lưu lượng truy cập. Trong trường hợp Wi-Fi Direct này có nghĩa là sẽ phải kết nối đến và ghép cặp với mỗi trong số các thiết bị khác riêng biệt. Điều này rất cồng kềnh, đặc biệt là nếu có nhiều thiết bị có liên quan. Ví dụ, đối với nền không dây của thiết bị mang được với nhiều thiết bị ngoại vi không dây, sẽ không thân thiện người sử dụng nếu người dùng cần phải thực hiện bước ghép cặp người sử dụng với thiết bị ngoại vi không dây riêng biệt. Do đó, điều quan trọng là giữ được lượng hoạt động ghép cặp đến mức tối thiểu.

Công nghệ TDLS, được biết đến từ "IEEE Std 802.1 Part 11 LZ-2010: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification, Amendmnet 7: Extensions to Direct-Link Setup (DLS), được xuất bản bởi IEEE ngày 14 tháng mười năm 2010", là một tùy chọn Wi-Fi cho phép thiết lập liên kết trực tiếp giữa hai thiết bị mà đã kết nối với cùng AP Wi-Fi, mà không cần phải ghép cặp để thiết lập kết nối trực tiếp bảo mật. Điều này được thực hiện như sau. Khi một thiết bị WiFi có khả năng TDLS được kết nối với AP, nó có thể gửi yêu cầu đến thiết bị có khả năng TDLS khác được kết nối với cùng một AP để thiết lập kết nối trực tiếp. Sau khi trao đổi thông tin như thông tin bằng chứng tin cậy bảo mật và thông tin về kênh Wi-Fi để sử dụng, hai thiết bị này có thể bắt đầu liên kết trực tiếp bảo mật riêng giữa hai thiết bị.

Tuy nhiên, TDLS có một số nhược điểm:

Tất cả các thiết bị có liên quan phải hỗ trợ hoạt động đồng thời (để duy trì liên kết trực tiếp đến thiết bị khác và liên kết đến AP cùng một lúc, bao gồm cả hoạt động trên hai tần số khác nhau), trong khi đó nhiều thiết bị ngoại vi mang được và không dây chỉ có thể thiết lập và duy trì kết nối Wi-Fi duy nhất và/hoặc kết nối Wi-Fi tần số duy nhất.

TDLS có một số vấn đề tương thích khi sử dụng trong mạng Wi-Fi Direct (ví dụ như TDLS thông qua Wi-Fi Direct GO để thiết lập liên kết trực tiếp giữa các thiết bị khác nhau bên trong nhóm Wi-Fi Direct P2P). Ví dụ, cơ cấu tiết kiệm công suất của Wi Fi Direct và TDLS không tương thích và có thể gây ra xung đột.

Việc trao đổi bằng chứng tin cậy bảo mật cho liên kết trực tiếp TDLS được thực hiện thông qua việc bắt tay TDLS Peer Key (khóa ngang hàng). Vấn đề là cái bắt tay giữa hai thiết bị TDLS được thực hiện thông qua AP. Do AP có thể giải mã thông điệp của các thiết bị TDLS liên quan, có nghĩa là AP có thể nghe lỏm được cái bắt tay này, và có khả năng phục hồi khóa mà thiết bị TDLS đồng ý cho kết nối trực tiếp. Khi chế độ PSK được sử dụng, thiết bị khác cũng gắn với cùng AP sẽ có thể nghe lỏm được lưu lượng truy cập này, ví dụ như, theo các cách sau đây: khi thiết bị Wi-Fi liên kết với AP sử dụng PSK, nó sử dụng mật khẩu và thông tin khác trong cái bắt tay Four-Way Handshake để tạo ra/lấy được khóa liên kết được gọi là khóa tạm thời ghép cặp (Pairwise transient key-PTK). PTK được sử dụng để mã hóa và xác thực của lưu lượng giữa thiết bị Wi-Fi và AP. Lưu lượng cho thiết bị khác được tái mã hóa bởi AP với PTK mà AP và thiết bị khác đã tạo ra từ Passphrase. Mặc dù AP có PTK khác nhau cho mỗi thiết bị Wi-Fi liên quan, thiết bị bất kỳ kết hợp với AP, mà có Passphrase, có thể tính được PTK mà được sử dụng bằng cách lắng nghe Four-Way Handshake giữa thiết bị khác và AP. Do bằng cách sử dụng PTK này, thiết bị có thể giải mã truyền thông giữa thiết bị khác và AP, điều này có nghĩa rằng nó cũng có thể nghe cái bắt tay TDLS Peer Key, và tính toán các khóa được sử dụng để bảo vệ liên kết trực tiếp TDLS giữa hai thiết bị TDLS. Do đó, TDLS theo mặc định không cung cấp truyền thông riêng bảo mật qua liên kết trực tiếp.

Việc ghép cặp thiết bị không dây và thiết lập kết nối luôn luôn phải đi qua điểm truy cập mà tất cả thiết bị trong nhóm phải được kết nối đến. Không thể kết nối trực tiếp với bất kỳ máy khách/trạm nào (ví dụ như màn hình hiển thị) trong nhóm trừ khi đầu tiên thiết lập kết nối với chủ điểm truy cập/nhóm. Điều này có nghĩa rằng có thể cần phải

được gần về mặt vật lý với chủ điểm truy cập/nhóm để thực hiện bước ghép cặp, do không thể kết nối với nhóm thông qua một trong số các thiết bị khác trong nhóm.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là cung cấp hệ thống truyền thông bảo mật mà giữ số lượng bước ghép cặp người sử dụng ở mức tối thiểu, ngăn chặn việc nghe trộm các liên kết trực tiếp giữa các thiết bị, và cung cấp sự linh hoạt trong việc kết nối với nhóm.

Với mục đích này, sáng chế đề xuất trong hệ thống truyền thông không dây như được mô tả trong đoạn mở đầu, thiết bị mang được bao gồm bộ xử lý truyền thông thiết bị để thiết lập kết nối bảo mật thứ hai với thiết bị không dây thứ hai cung cấp chức năng máy chủ thứ hai sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai khác với dữ liệu bí mật thứ nhất, nhận lệnh thứ hai thông qua kết nối bảo mật thứ hai, và, theo lệnh thứ hai, thiết lập kết nối bảo mật không dây trực tiếp tương ứng với ít nhất một thiết bị không dây của nhóm sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba, dữ liệu bí mật thứ ba khác với dữ liệu bí mật thứ nhất; thiết bị không dây thứ hai cung cấp chức năng máy chủ thứ hai bao gồm bộ xử lý truyền thông máy chủ để thiết lập kết nối bảo mật thứ hai với thiết bị mang được sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai, chuyển đến ít nhất một thiết bị không dây thông qua kết nối bảo mật thứ nhất lệnh thứ nhất để áp dụng dữ liệu bí mật thứ ba cho việc thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được, và chuyển đến thiết bị mang được thông qua kết nối bảo mật thứ hai lệnh thứ hai để áp dụng dữ liệu bí mật thứ ba cho việc thiết lập kết nối bảo mật không dây trực tiếp với ít nhất một thiết bị không dây dựa trên dữ liệu bí mật thứ ba; ít nhất một thiết bị không dây bao gồm bộ xử lý truyền thông để nhận lệnh thứ nhất thông qua kết nối bảo mật thứ nhất, và, theo lệnh thứ nhất, thiết lập kết nối bảo mật không dây trực tiếp tương ứng với thiết bị mang được bằng cách sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba.

Với mục đích này, theo một khía cạnh khác, sáng chế đề xuất phương pháp truyền thông không dây trong hệ thống thiết bị không dây như được mô tả trong phần mở đầu bao gồm bước thiết lập kết nối bảo mật thứ hai giữa thiết bị mang được và thiết bị không dây thứ hai cung cấp chức năng máy chủ thứ hai sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai khác với dữ liệu bí mật thứ nhất; chuyển đến ít nhất một thiết bị không dây của nhóm thông qua kết nối bảo mật thứ nhất lệnh thứ nhất áp dụng dữ liệu bí mật

thứ ba cho việc thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được, dữ liệu bí mật thứ ba khác với dữ liệu bí mật thứ nhất (240), và chuyển đến thiết bị mang được thông qua kết nối bảo mật thứ hai lệnh thứ hai để áp dụng dữ liệu bí mật thứ ba cho việc thiết lập kết nối bảo mật không dây trực tiếp với ít nhất một thiết bị không dây dựa trên dữ liệu bí mật thứ ba; thiết lập kết nối trực tiếp bảo mật không dây tương ứng giữa thiết bị mang được và ít nhất một thiết bị không dây sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba.

Các phần tử chính của hệ thống bảo mật và phương pháp cho phép thiết bị mang được A (ví dụ như thiết bị tương thích Wi-Fi Direct) kết nối với nhóm G các thiết bị không dây. Nhóm G được cấu hình sẵn để hoạt động như nhóm được kết nối với thiết bị không dây có sức cung cấp chức năng máy chủ thứ nhất và chia sẻ bí mật chung S1 được sử dụng để đảm bảo truyền thông bên trong nhóm. Nhóm này có thể, ví dụ, bao gồm máy chủ nền không dây và thiết bị ngoại vi không dây. Thiết bị A kết nối với một trong số các thiết bị không dây, có chức năng như thiết bị máy chủ thứ hai cung cấp chức năng máy chủ thứ hai, trong nhóm sử dụng bí mật S2 cho việc đảm bảo truyền thông thông qua kết nối bảo mật thứ hai. Sau đó, các thiết bị trong nhóm và thiết bị A được lệnh về bí mật S3, tiếp theo là thiết bị A để bắt đầu lắng nghe kết nối gửi đến, theo sau bởi một hoặc nhiều thiết bị thiết lập kết nối không dây bảo mật trực tiếp với thiết bị A sử dụng bí mật S3 để tự động ghép cặp với thiết bị A, ví dụ như theo cách tương thích với Wi-Fi Direct. Tùy chọn, thiết bị máy chủ thứ hai là thiết bị tương tự như thiết bị không dây cung cấp chức năng máy chủ thứ nhất.

Do đó, chức năng máy chủ thứ nhất và thứ hai có thể được thực hiện trong một thiết bị không dây duy nhất. Hơn nữa, nhóm G có thể bao gồm thiết bị mà chỉ có khả năng hỗ trợ một vai trò P2P Client hoặc một trạm Wi-Fi (STA), và không phải là chủ nhóm P2P hoặc vai trò AP Wi-Fi.

Các biện pháp có hiệu quả mà hệ thống truyền thông bảo mật không dây và giao thức bảo mật được cung cấp để phân phối các bí mật được sử dụng để thiết lập liên kết trực tiếp bảo mật với số bước ghép cặp người sử dụng ít nhất, theo cách có thể ngăn chặn việc nghe trộm các liên kết trực tiếp giữa các thiết bị, và ngoài ra còn cung cấp sự linh hoạt hơn bằng cách cho phép thiết bị bất kỳ có khả năng thực hiện chức năng máy chủ thứ hai là điểm vào nhóm thiết bị không dây thực hiện chức năng. Ví dụ, nhóm thiết bị có thể cung cấp môi trường nền cho thiết bị mang được, như điện thoại thông minh. Cụ thể,

các thiết bị nền không luôn luôn phải sử dụng cùng thiết bị trong hệ thống nền (ví dụ như một AP hoặc GO) để kết nối với nhóm, mà thay vào đó có thể kết nối với thiết bị bất kỳ nào trong nhóm cung cấp chức năng máy chủ thứ hai.

Sáng chế cũng dựa trên sự thừa nhận sau đây (bằng cách sử dụng môi trường Wi-Fi làm một ví dụ). Khi nhóm thiết bị Wi-Fi Direct cùng nhau thực hiện chức năng cho thiết bị không dây (như đưa vào nhóm không dây), mong muốn là thiết bị không dây khác có thể thiết lập một hoặc nhiều liên kết ngang hàng với thiết bị không dây bất kỳ trong nhóm mà không cần phải thực hiện hành động ghép cặp người sử dụng với mỗi thiết bị này trong nhóm một cách riêng biệt.

Wi-Fi Direct có khái niệm về chủ sở hữu nhóm (GO). Nếu tất cả các thiết bị Wi-Fi trong nhóm sẽ kết nối với cùng GO, và GO hỗ trợ cái gọi là tính năng phân phối Intra BSS (trong nội bộ BSS) của Wi-Fi Direct, thì việc làm đủ là thiết bị không dây khác kết nối đến GO để có thể giao tiếp với tất cả các thiết bị trong nhóm. Lĩnh vực phân phối Intra-BSS cho biết nếu thiết bị P2P đang là máy chủ, hay có ý định là máy chủ, nhóm P2P mà cung cấp dịch vụ phân phối dữ liệu giữa các máy khách trong nhóm P2P. Tuy nhiên, tất cả truyền thông sẽ phải đi qua GO này. Điều này là rất không hiệu quả, và làm tăng độ trễ truyền thông. Đối với chức năng như kết hợp vào nhóm không dây, độ trễ là một vấn đề quan trọng. Kết nối với màn hình hiển thị không dây, chuột, bàn phím, v.v. cần có độ trễ càng thấp càng tốt. Vì vậy, điều quan trọng là có thể thiết lập kết nối trực tiếp (tức là ngang hàng) với nhiều hoặc thậm chí tất cả các thành viên của nhóm. Tuy nhiên, điều này đòi hỏi nhiều bước ghép cặp người sử dụng được thực hiện cho mỗi thiết bị được đưa vào nhòm không dây mà muốn kết nối vào nhóm thiết bị ngoại vi này. Vì các lý do đã đề cập trong phần trước, sử dụng TDLS không phải là một lựa chọn để khắc phục vấn đề này.

Một vấn đề khác là Wi-Fi Direct áp đặt những hạn chế nhất định lên các thiết bị, chẳng hạn như hạn chế là thiết bị P2P chỉ có thể được kết nối với một GO duy nhất. Sau khi kết nối với một GO, thiết bị P2P thay đổi vai trò, tức là thiết bị này trở thành máy khách P2P. Wi-Fi Direct xác định các hạn chế khác nhau cho máy khách P2P, như hạn chế về khả năng phát hiện và giao tiếp giữa các máy khách P2P. Hơn nữa, số lượng các trường hợp máy khách P2P đồng thời mà thường có thể chạy trên thiết bị duy nhất cũng rất hạn chế. Nhiều thiết bị ngoại vi không dây cấp thấp (như chuột hoặc bàn phím Wi-Fi) được dự kiến thậm chí còn có hạn chế khác nữa do những hạn chế về tài nguyên của

chúng, chẳng hạn như, chỉ hỗ trợ vai trò máy khách P2P và chỉ hỗ trợ một liên kết Wi-Fi duy nhất.

Sáng chế khắc phục các vấn đề trên bằng giao thức bảo mật mà tạo ra, thông qua máy chủ thứ hai, dữ liệu bí mật thứ ba và chỉ thị thiết bị mang được (thiết bị được kết nạp- thiết bị được nhận vào hoạt động không dây) và các thiết bị không dây của nhóm để áp dụng dữ liệu bí mật thứ ba để kết nối thiết bị thứ nhất với thiết bị không dây được lựa chọn của nhóm, ví dụ như, tạo thành môi trường kết nạp cấu hình sẵn.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thiết bị còn được bố trí để kiểm soát truyền thông qua kết nối không dây trực tiếp như là chủ nhóm. Nói chung, trong hệ thống mạng không dây, thiết bị có thể điều khiển nhóm thiết bị như là chủ nhóm, ví dụ như, trong WLAN thực hiện vai trò AP. Trong một ví dụ trong Wi-Fi, thiết bị thứ nhất nhận vai trò chủ nhóm Wi-Fi Direct khi thiết lập kết nối Wi-Fi Direct P2P giữa các thiết bị trong tập con G' của các thiết bị không dây xa hơn và thiết bị thứ nhất.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thiết bị còn được bố trí để thiết lập kết nối bảo mật không dây trực tiếp khác nhau tương ứng với thiết bị không dây tương ứng của các tập con khác nhau tương ứng bằng cách sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba khác nhau tương ứng. Thuận lợi nếu, các tập con được chứa để giao tiếp với thiết bị thứ nhất thông qua các thể hiện khác nhau của dữ liệu bí mật thứ ba.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thiết bị còn được bố trí để nhận lệnh thứ hai bao gồm dữ liệu bí mật thứ ba khác nhau tương ứng cho nhiều tập con. Thuận lợi nếu, các tập con được chứa để giao tiếp với thiết bị mang được thông qua một lệnh duy nhất.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thiết bị còn được bố trí để tạo ra dữ liệu bí mật thứ ba và chuyển dữ liệu bí mật thứ ba này đến thiết bị cung cấp chức năng máy chủ thứ hai. Thuận lợi nếu, thiết bị mang được kiểm soát bảo mật bằng cách kiểm soát việc tạo ra dữ liệu bí mật thứ ba.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thứ nhất còn được bố trí để ngắt kết nối kết nối bảo mật thứ hai trước khi bắt đầu thiết lập kết nối bảo mật không dây trực tiếp tương ứng với thiết bị không dây tương ứng của các tập con. Thuận lợi nếu, khả năng của bộ thu phát rađio ít hơn cần đến và khả năng thấp hơn của phương tiện không dây được sử dụng.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thiết bị còn được bố trí để cung cấp nhóm vĩnh cửu, và do đó, sau khi ngắt kết nối bảo mật không dây trực tiếp tương ứng dựa trên dữ liệu bí mật thứ ba, thực hiện thiết lập kết nối bảo mật trực tiếp không dây thêm nữa tương ứng dựa trên dữ liệu bí mật thứ ba. Thuận lợi nếu, khi thiết bị mang được, ví dụ như, thiết bị được đưa vào nhóm, kết nối lại, truyền thông bảo mật được phục hồi nhanh hơn.

Tùy chọn, trong thiết bị mang được, bộ xử lý truyền thông thiết bị còn được bố trí cho việc sử dụng dữ liệu bí mật thứ hai hoặc dữ liệu bí mật thứ ba thu được trước đó, khi ghép cặp, sau khi ngắt kết nối kết nối bảo mật không dây trực tiếp tương ứng dựa trên dữ liệu bí mật thứ ba này, kết nối lại với thiết bị không dây tương ứng của các tập con để thiết lập kết nối bảo mật không dây trực tiếp tương ứng. Thuận lợi, khi thiết bị mang được, ví dụ như thiết bị được đưa vào nhóm, kết nối lại, truyền thông bảo mật được phục hồi nhanh hơn.

Tùy chọn, kết nối bảo mật thứ hai bao gồm kết nối Wi-Fi Direct P2P. Trong thực tế, kết nối này có thể là kết nối Wi-Fi Direct P2P và trong đó dữ liệu bí mật thứ hai (S2) là Passphrase (mật khẩu) Wi-Fi, ví dụ như PMK (khóa chính ghép cặp) Wi-Fi hoặc PSK Wi-Fi.

Tùy chọn, kết nối bảo mật không dây trực tiếp tương ứng bao gồm kết nối Wi-Fi Direct ngang hàng, và/hoặc kết nối bảo mật không dây trực tiếp tương ứng bao gồm kết nối TDLS. Trong thực tế, kết nối trực tiếp giữa các thiết bị trong nhóm G' và thiết bị thứ nhất có thể là kết nối Wi-Fi Direct P2P và trong đó dữ liệu bí mật thứ ba là mật khẩu Wi-Fi, ví dụ như PMK (khóa chính theo cặp) Wi-Fi hoặc PSK Wi-Fi. Ngoài ra, kết nối trực tiếp giữa các thiết bị trong nhóm G' và thiết bị thứ nhất là kết nối TDLS. Hơn nữa, thủ tục ghép cặp có thể bao gồm truy cập Wi-Fi được bảo vệ (WPA/WPA2) hoặc thủ tục cấu hình đơn giản Wi-Fi. Thuận lợi nếu, thủ tục ghép cặp được biết này có thể đã có sẵn trong thiết bị không dây, và có thể được chia sẻ.

Tùy chọn, bước cấu hình trước bao gồm việc chỉ định thiết bị cung cấp chức năng máy chủ thứ hai để có chủ sở hữu nhóm Wi-Fi Direct P2P của nhóm P2P bao gồm thiết bị máy chủ thứ hai và thiết bị trong nhóm G, và ghép cặp từng thiết bị trong nhóm này với thiết bị máy chủ thứ hai để có được bí mật S1 chung từ thiết bị máy chủ thứ hai và trong đó S1 là mật khẩu PMK Wi-Fi hoặc PSK WiFi.

Tùy chọn, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được sắp xếp để tạo ra dữ liệu bí mật thứ ba. Thuận lợi nếu, thiết bị máy chủ kiểm soát bảo mật bằng cách kiểm soát việc tạo ra dữ liệu bí mật thứ ba.

Tùy chọn, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được sắp xếp để tạo ra tập khác nhau tương ứng của dữ liệu bí mật thứ ba cho các thể hiện khác nhau tương ứng của thiết bị thứ nhất. Thuận lợi nếu, việc nghe lỏm truyền thông được ngăn giữa các thiết bị thứ nhất khác nhau.

Tùy chọn nếu, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được sắp xếp để tạo ra tập khác nhau tương ứng dữ liệu bí mật thứ ba khi thiết bị (A), sau khi đã ngắt kết nối bảo mật thứ hai, đang thiết lập kết nối bảo mật thứ hai ở thời gian tương ứng sau đó. Thuận lợi nếu, cuộc tấn công phát lại tránh được bằng cách tạo ra các tập khác nhau của dữ liệu bí mật thứ ba.

Tùy chọn, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được sắp xếp để tạo ra tập khác nhau tương ứng của dữ liệu bí mật thứ ba cho tập khác nhau tương ứng của thiết bị không dây trong nhóm. Thuận lợi nếu, nhiều tập con được chứa để giao tiếp với thiết bị thứ nhất thông qua các thể hiện khác nhau của dữ liệu bí mật thứ ba.

Tùy chọn, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được sắp xếp để tạo ra dữ liệu bí mật thứ ba dựa trên, hoặc bằng với, dữ liệu bí mật thứ hai. Về cơ bản, dữ liệu bí mật thứ ba có thể được lựa chọn khác với dữ liệu bí mật thứ hai, có tăng cường bảo mật. Thuận lợi nếu, dữ liệu bí mật thứ ba có thể được tạo ra dựa trên dữ liệu bí mật thứ hai, mà tăng cường tính hiệu quả. Ngoài ra, dữ liệu bí mật thứ ba có thể được lựa chọn bằng với dữ liệu bí mật thứ hai, mà tăng cường tốc độ do ít dữ liệu cần phải được chuyển.

Tùy chọn, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được bố trí để gán tuổi đời hạn chế cho dữ liệu bí mật thứ ba, và/hoặc gán tuổi đời cho dữ liệu bí mật thứ ba tùy thuộc vào mức độ được phép của thiết bị (A). Thuận lợi nếu, việc truy cập hệ thống bảo mật được giới hạn theo thời gian, hay máy khách hoặc chủ sở hữu có thể được gán các quyền khác nhau.

Tùy chọn, trong thiết bị máy chủ, bộ xử lý truyền thông máy chủ được sắp xếp để chuyển lệnh thứ ba đến thiết bị không dây tương ứng của các tập con để ngắt kết nối kết nối bảo mật thứ nhất trước khi thiết lập kết nối bảo mật không dây trực tiếp tương ứng

với thiết bị. Thuận lợi nếu, ít khả năng của bộ thu phát rađio hơn cần thiết và khả năng thấp hơn của phương tiện không dây được sử dụng.

Tùy chọn, thiết bị máy chủ là máy chủ không dây hoặc trạm không dây. Trong thực tế, thiết bị máy chủ có thể là cùng thiết bị như thiết bị máy chủ không dây thứ nhất và/hoặc thiết bị máy chủ không dây thứ hai. Do đó, chức năng máy chủ thứ nhất và thứ hai có thể được thực hiện trong một máy chủ nhận hoạt động duy nhất hoặc trạm nhận hoạt động không dây.

Tùy chọn, trong thiết bị không dây, bộ xử lý truyền thông tương ứng được bố trí để khởi tạo việc thành lập kết nối bảo mật không dây trực tiếp đến thiết bị mang được. Thuận lợi nếu, thiết bị không dây điều khiển các thiết lập.

Tùy chọn, trong thiết bị không dây, bộ xử lý truyền thông tương ứng được bố trí để ngắt kết nối kết nối bảo mật thứ nhất trước khi thiết lập kết nối bảo mật không dây trực tiếp tương ứng đến thiết bị mang được. Thuận lợi nếu, ít khả năng của bộ thu phát rađio cần đến và khả năng thấp hơn của phương tiện không dây được sử dụng.

Tùy chọn, trong thiết bị không dây, bộ xử lý truyền thông tương ứng được bố trí cho việc khôi phục kết nối bảo mật thứ nhất sau khi ngắt kết nối kết nối bảo mật không dây trực tiếp tương ứng đến thiết bị mang được. Thuận lợi nếu, nhóm cấu hình sẵn sẽ tự động kết nối lại sau khi thiết bị thứ nhất đã được ngắt kết nối.

Tùy chọn, thiết bị máy chủ có khả năng là một phần của hai nhóm Wi-Fi Direct P2P độc lập, một nhóm bao gồm các thiết bị trong nhóm G, và nhóm kia bao gồm thiết bị mang được có kết nối P2P đến thiết bị máy chủ.

Tùy chọn, thiết bị máy chủ thông báo cho các thiết bị khác trong nhóm G về bí mật S3 trước khi thiết bị mang được A kết nối. Thuận lợi nếu, kết nối của thiết bị mang được vào nhóm, ví dụ như các thủ tục đưa vào nhóm, được thực hiện nhanh hơn.

Tùy chọn, thiết bị máy chủ hỗ trợ hoạt động nhóm vĩnh cửu Wi-Fi Direct. Tùy chọn, thiết bị máy chủ mời các thiết bị trong nhóm G để kết nối với thiết bị máy chủ bằng cách sử dụng các thủ tục mời Wi-Fi Direct P2P. Tùy chọn, thủ tục ghép cặp tự động dựa trên truy cập Wi-Fi được bảo vệ (ví dụ như WPA hoặc WPA2). Tùy chọn, thủ tục ghép cặp tự động dựa trên cấu hình đơn giản Wi-Fi. Tùy chọn, thiết bị mang được hỗ trợ phân phối bên trong BSS Wi-Fi Direct để thiết bị không dây trong nhóm G vẫn có thể giao tiếp với nhau để thực hiện chức năng với nhau, mà không đòi hỏi đường trục. Tùy chọn, thiết bị mang được hỗ trợ hoạt động nhóm Wi-Fi Direct vĩnh cửu, và sử dụng dữ liệu bí mật

thứ ba lấy ra từ kết nối thứ nhất với nhóm thông qua thiết bị máy chủ thứ hai để kết nối với thiết bị của tập con trong kết nối tiếp theo. Thuận lợi nếu, các tùy chọn này là sự mở rộng của các phần tử hiện có của thiết bị Wi-Fi.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ thể hiện hệ thống nhận vào hoạt động không dây trong khi cấu hình trước;

Fig.2 là sơ đồ thể hiện thiết bị không dây thiết lập kết nối đến máy chủ;

Fig.3 là sơ đồ thể hiện máy chủ không dây lệnh thiết bị không dây đã kết nối; và

Fig.4 là sơ đồ thể hiện thiết bị không dây kết nối trực tiếp đến các thiết bị không dây khác nữa.

Mô tả chi tiết sáng chế

Một ví dụ thực hiện chi tiết hệ thống nhận vào hoạt động không dây được mô tả dưới đây. Việc nhận vào hoạt động không dây có nghĩa là cho phép thiết bị mang được (thiết bị này được gọi là thiết bị được chấp nhận hoạt động không dây hoặc WD) kết nối không dây với nhóm thiết bị ngoại vi không dây, do đó các ứng dụng trên thiết bị mang được có thể sử dụng các thiết bị ngoại vi này để nâng cao trải nghiệm và năng suất làm việc/tương tác với các ứng dụng này. Việc nhóm lại các thiết bị ngoại vi, việc phát hiện nhóm thiết bị ngoại vi, quản lý kết nối đến các nhóm thiết bị ngoại vi, được thực hiện bởi bộ phận được gọi là máy chủ nhận vào hoạt động không dây (WDH).

Thiết bị được chấp nhận hoạt động không dây có thể bao gồm (nhưng không giới hạn ở) điện thoại di động, máy tính xách tay, máy tính bảng, máy phát phương tiện truyền thông, máy ảnh. WDH có thể bao gồm (nhưng không giới hạn ở) thiết bị trạm nhận vào hoạt động không dây dành riêng, thiết bị hiển thị, thiết bị âm thanh, máy in, máy tính cá nhân. Thiết bị ngoại vi có thể bao gồm (nhưng không giới hạn ở) những chuột không dây, bàn phím, màn hình hiển thị, thiết bị âm thanh, webcam, máy in, thiết bị máy chủ, USB. Thiết bị ngoại vi được coi là để hỗ trợ các tiêu chuẩn như Wi-Fi Serial Bus và Wi-Fi Display để làm cho chức năng của chúng khả dụng thông qua mạng không dây đến các thiết bị khác như thiết bị được chấp nhận không dây và WDH. Thiết bị ngoại vi có dây có thể được kết nối với mạng không dây bằng cách kết nối chúng vào thiết bị trung gian thông qua dây, và thiết bị trung gian có khả năng kết nối không dây như được định nghĩa

trong tài liệu này, ví dụ như, hub USB có hỗ trợ Wi-Fi Serial Bus. Thiết bị ngoại vi và thiết bị được chấp nhận hoạt động không dây bản thân chúng cũng có thể là WDH.

Fig.1 thể hiện hệ thống nhận vào hoạt động không dây trong khi cấu hình trước. Hệ thống nhận vào hoạt động không dây có thiết bị máy chủ nhận vào hoạt động không dây H 100, và một số thiết bị ngoại vi không dây P1 ... Pn 110, 120, 130, 140. Tất cả các thiết bị này đều có bộ thu phát rađio Wi-Fi 101, 111 và hỗ trợ tham gia vào nhóm Wi-Fi Direct P2P. Một số thiết bị ngoại vi có thể bị giới hạn chỉ ở chỗ hỗ trợ hoạt động là máy khách P2P hoặc máy khách kế thừa.

Fig.1 thể hiện tình huống ban đầu cấu hình trước tập thiết bị ngoại vi để nhận vào hoạt động không dây. Các thiết bị ngoại vi tạo thành nhóm 190 các thiết bị không dây mà được kết nối với thiết bị máy chủ H 100 thông qua kết nối Wi-Fi trực tiếp 150 SC1 ... SCn, hoạt động như chủ sở hữu nhóm (P2P GO) của nhóm P2P được tạo thành bởi H và các thiết bị ngoại vi P1 ... Pn hoạt động như máy khách P2P. Nhờ đó, thiết bị không dây có bộ xử lý truyền thông tương ứng 112, được thể hiện có chức năng của máy khách P2P. Trong thực tế, bộ xử lý truyền thông của thiết bị không dây này và/hoặc thiết bị máy chủ được biết là có thể được cài đặt trong mạch tích hợp chuyên dụng, trong mạch có thể lập trình và/hoặc trong phần sụn mà được thực thi trên vi điều khiển hoặc bộ xử lý chuyên dụng. Các bộ xử lý truyền thông được bố trí để thực hiện quá trình truyền thông như được giải thích dưới đây.

Việc thiết lập kết nối Wi-Fi Direct SC1 ... SCn đòi hỏi bước ghép cặp, ví dụ như sử dụng cấu hình đơn giản Wi-Fi (WSC). Trong bước ghép cặp này, bí mật chung S1 được cung cấp bởi H để thiết lập kết nối bảo mật dựa trên truy cập Wi-Fi được bảo vệ (WPA/WPA2). Bí mật S1 có thể là mật khẩu (PMK Wi-Fi hoặc PSK Wi-Fi), được sử dụng trong cuộc bắt tay bốn bên để thiết lập truy cập Wi-Fi được bảo vệ (WPA/WPA2).

Có rất nhiều khả năng để phân phối bí mật S1, ví dụ như bí mật S1 có thể được phân phối sử dụng cấu hình đơn giản Wi-Fi hoặc bí mật S1 có thể được cấu hình sẵn trong tất cả các thiết bị có liên quan. Thiết bị máy chủ nhận vào hoạt động không dây H cũng có bộ xử lý truyền thông máy chủ 102 (còn gọi là quản lý nhận vào hoạt động không dây) để lưu trữ thông tin về thiết bị ngoại vi, theo dõi kết nối, thiết lập bí mật, lệnh các thiết bị khác, cấu hình mà các thiết bị ngoại vi cùng với nhau tạo thành môi trường nhận vào hoạt động không dây.

Fig.2 thể hiện thiết bị không dây thiết lập kết nối đến một máy chủ. Thiết bị không dây 200 được gọi là thiết bị được nhận vào hoạt động không dây D và được thể hiện trong hệ thống nhận vào hoạt động không dây tương tự như được thể hiện trên Fig.1 ở trên. Thiết bị không dây có bộ thu phát Wi-Fi rađio 201 và bộ xử lý truyền thông PROC 202 để kiểm soát quá trình truyền thông.

Trong hệ thống này, thiết bị được nhận vào hoạt động không dây D thiết lập kết nối Wi-Fi Direct C 250 với máy chủ nhận vào hoạt động không dây H 210 để nhận tập thiết bị ngoại vi. Ví dụ cụ thể này chỉ cho thấy giải pháp mà theo đó thiết bị được nhận vào hoạt động không dây thiết lập kết nối nhận vào hoạt động không dây ban đầu (cái được gọi là kết nối giám sát và điều khiển) đến máy chủ nhận vào hoạt động không dây H và không đến bất cứ thiết bị P1 ... Pn nào. Cần lưu ý rằng, tương tự, các thiết bị được nhận vào hoạt động không dây có thể thiết lập kết nối ban đầu với thiết bị bất kỳ trong các thiết bị không dây Pl...Pn, khi thiết bị không dây đó được bố trí để thực hiện chức năng máy chủ để thiết lập kết nối ban đầu. Do đó, chức năng máy chủ có thể được thực hiện bởi thiết bị duy nhất, hoặc có thể được phân phối giữa các thiết bị khác nhau.

Trong các bước ghép cặp giữa D và H để thiết lập kết nối C, H chắc chắn rằng vì lý do bảo mật bí mật S2 khác với S1 được cung cấp bởi H để thiết lập kết nối bảo mật dựa trên truy cập Wi-Fi được bảo vệ (WPA/WPA2). Tương tự như kết nối SC1 ... SCn dựa trên dữ liệu bí mật S1 như được chỉ ra bởi các đường kết nối 240, bí mật S2 là mật khẩu (PMK Wi-Fi hoặc PSK Wi-Fi), được sử dụng trong khi bắt tay bốn bên để thiết lập truy cập Wi-Fi được bảo vệ (WPA/WPA2).

Có rất nhiều khả năng để phân phối bí mật S2, ví dụ như bí mật S2 có thể được phân phối sử dụng cấu hình đơn giản Wi-Fi hoặc bí mật S2 có thể được cấu hình sẵn trong tất cả thiết bị có liên quan. Trong ví dụ này, D kết nối với H của P2P GO, theo đó D sẽ tự động trở thành máy khách P2P. Ngoài ra, D và H tạo thành nhóm P2P mới, độc lập với nhóm P2P được thiết lập giữa H và thiết bị ngoại vi, nhờ đó hoặc D hoặc H có thể trở thành P2P GO.

Fig.3 thể hiện máy chủ lưu trữ không dây lệnh thiết bị không dây được kết nối. Máy chủ không dây H 310 được thể hiện trong hệ thống nhận vào hoạt động không dây tương tự như được thể hiện trên Fig.1 và Fig.2 ở trên. Hình vẽ này thể hiện thiết bị được nhận vào hoạt động không dây D 200 và thiết bị ngoại vi P1 .. .Pn 110, 120 nhận lệnh từ máy chủ nhận vào hoạt động không dây H 310.

Hình vẽ thể hiện rằng H chỉ thị một hoặc nhiều thiết bị ngoại vi thông qua các lệnh I1, v.v.. Trong 320, và cũng là thiết bị được nhận vào hoạt động không dây thông qua lệnh D1 330, về việc sử dụng bí mật S3 trong bước ghép cặp tự động giữa thiết bị ngoại vi và D. Các lệnh và tin nhắn này có thể có định dạng bất kỳ bằng cách sử dụng nhiều giao thức truyền thông khác nhau, từ các lệnh mã hóa nhị phân trong khung MAC đến các lệnh mã hóa XML trên HTTP.

Ngoài dữ liệu bí mật S3, các lệnh cũng có thể bao gồm thông tin về hành động nào mà thiết bị cần phải thực hiện sau khi nhận được chúng, chẳng hạn như, ngắt kết nối với H và thiết lập kết nối với D. Thiết bị ngoại vi có thể cần phải được cung cấp thông tin về SSID (Service Set Identifier – định danh tập dịch vụ) mà D sẽ sử dụng để quảng cáo khả năng Wi-Fi Direct của nó, và D có thể cần phải được cung cấp thông tin như định danh duy nhất của thiết bị ngoại vi mà sẽ thiết lập kết nối. Một hoặc nhiều thiết bị ngoại vi Pi cũng có thể duy trì kết nối với H. Thiết bị này có thể nhận lệnh để duy trì kết nối với H, hoặc để ngắt kết nối từ H. Như được thể hiện trên Fig.3, giả định rằng thiết bị P3 ... Pn-1 nhận lệnh để duy trì kết nối với H.

Sử dụng kênh C, được bảo vệ bởi khóa được tạo ra từ dữ liệu bí mật S2, dữ liệu bí mật S3 cũng được gửi đến thiết bị được nhận vào hoạt động không dây D. Điều này có nghĩa rằng D và một hoặc nhiều thiết bị ngoại vi có thể thiết lập kết nối được bảo vệ WPA/WPA2 trực tiếp bằng cách sử dụng bắt tay bốn bên và việc thi hành thủ tục cấu hình đơn giản Wi-Fi, liên quan đến tương tác người dùng có thể khi nhập mã PIN, không cần thiết. Việc không phải thực hiện thủ tục cấu hình đơn giản Wi-Fi cũng tăng tốc độ quá trình nhận vào hoạt động không dây.

Fig.4 thể hiện thiết bị không dây kết nối trực tiếp đến các thiết bị không dây khác. Thiết bị không dây D 400 được thể hiện trong hệ thống nhận vào hoạt động không dây tương tự như được thể hiện trên Fig.1, Fig.2 và Fig.3 ở trên. Hình vẽ này thể hiện thiết bị được nhận vào hoạt động không dây D 400 và tập con, ví dụ ba thiết bị ngoại vi 110, 120,140, thiết bị ngoại vi P1 .. .Pn đang được kết nối trực tiếp, và tùy chọn bị ngắt kết nối được chỉ ra bởi đường đứt nét 430 từ máy chủ nhận vào hoạt động không dây H 100. Trên Fig.1, thiết bị ngoại vi 130 không kết nối với thiết bị được nhận vào hoạt động không dây D và vẫn chỉ kết nối với máy chủ nhận vào hoạt động không dây 100.

Hình vẽ này cho thấy tình huống mà thiết bị P1, P2 và Pn đã thiết lập kết nối trực tiếp SP1, SP2 và SPn với thiết bị thiết bị được nhận vào hoạt động không dây D, sử dụng

dữ liệu bí mật S3 (mật khẩu S3) được chỉ ra bởi 420. D hoạt động như chủ sở hữu nhóm Wi-Fi Direct (được chỉ định bởi bộ phận P2P GO 403 trên hình vẽ) cho SD1, SD2 và SDn. Kết nối SC1, SC2 và SCn với H có thể được nhả ra hoặc có thể vẫn hoạt động. Các đường chấm trên Fig.4 phản ánh điều đó. Việc nhận vào hoạt động liên quan đến việc thiết bị được nhận vào hoạt động không dây D thay đổi vai trò và trở thành GO P2P cho tập con thiết bị ngoại vi không dây. Trong khi bắt tay bốn bên WPA/WPA2, S3 có thể được sử dụng như bí mật chung (PMK Wi-Fi hoặc PSK Wi-Fi) để tạo ra khóa liên kết (khóa tạm ghép cặp). Ngoài ra, S3 được sử dụng trong thủ tục ghép cặp thiết lập Wi-Fi được bảo vệ, trong đó thay vì người dùng nhập ví dụ như mã PIN, mã PIN được tạo ra từ S3.

Trong thực tế, hệ thống nhận vào hoạt động không dây trên có thể được áp dụng để kết nối thiết bị được nhận vào hoạt động không dây D trực tiếp với thiết bị hiển thị hoặc (USB), chuột/bàn phím để làm giảm độ trễ. Các thiết bị có thể được lệnh để sử dụng tập cấu hình được xác định trước. Các thiết bị bị ngắt kết nối có thể đi vào giấc ngủ. Tùy chọn, máy chủ không dây có thể ra lệnh để chúng thức dậy thường xuyên vào các khoảng thời gian cụ thể để có thể phát hiện ra chúng và kết nối với chúng một lần nữa.

Trong hệ thống làm ví dụ này, thiết bị ngoại vi không dây P (ví dụ như màn hình hiển thị Wi-Fi) có thể ban đầu được kết nối đến máy chủ không dây H thông qua kênh bảo mật C dựa trên khóa liên kết (khóa tạm ghép cặp) dựa trên mật khẩu S1. Máy chủ hoạt động như chủ sở hữu nhóm (GO) và P đóng vai trò máy khách. H và P cả hai cùng hỗ trợ việc nhóm P2P vĩnh cửu Wi-Fi Direct. Nhờ đó, P lưu trữ mật khẩu S1 trong bộ nhớ của nó. Thiết bị được nhận vào hoạt động không dây D ban đầu kết nối với máy chủ H thông qua Wi-Fi Direct trên kênh bảo mật với khóa liên kết (khóa tạm ghép cặp) mà dựa trên S2. Thông qua một giao thức cấu hình nhận vào hoạt động, H ra lệnh cho thiết bị được nhận vào hoạt động không dây D rằng kết nối tải qua Wi-Fi phải được chấp nhận. Kết nối trực tiếp với thiết bị ngoại vi P được thực hiện thông qua bộ phận chủ sở hữu nhóm tại D, trong khi sử dụng mật khẩu S3 để tạo ra khóa liên kết (khóa tạm ghép cặp) M theo thoả thuận với thiết bị ngoại vi P. H cũng chỉ thị cho P là nó phải kết nối với GO của thiết bị ngoại vi D trong khi sử dụng khóa liên kết (khóa tạm ghép cặp) M theo thoả thuận với D. Sau đó, P có thể ngắt kết nối với H và thiết lập liên kết với D với khóa liên kết (khóa tạm ghép cặp) M. Nếu kết nối bị đứt giữa P và D (ví dụ: nếu D không được nhận vào hoạt động không dây), thì P có thể kết nối lại với H sử dụng mật khẩu gốc S1.

Trong phương án thực tế, hệ thống nhận vào hoạt động không dây nâng cao như đã được mô tả ở trên có thể được thực hiện như sau. Trong hệ thống nhận vào hoạt động không dây này, có máy chủ không dây WDH thông qua đó thiết bị không dây WD có thể nhận vào hoạt động không dây. WDH được kết nối với thiết bị ngoại vi PF thông qua giao diện có dây và không dây và cũng có thể có PF được xây dựng sẵn. Giả định rằng một số trong số các PF không dây có chức năng bổ sung được xây dựng sẵn để chúng có thể được ra lệnh để kết nối trực tiếp đến WD đã được nhận vào hoạt động không dây, hoặc được trang bị để thực hiện chức năng máy chủ không dây.

Các ưu điểm sau đây đạt được bằng hệ thống nhận vào hoạt động không dây nâng cao. PF có thể nhanh chóng được kết nối với một WD (không cần phải thực hiện giao thức WSC - cấu hình kết nối Wi-Fi đơn giản), và không có sự can thiệp của người dùng. WD mà chỉ được phép nhận vào hoạt động không dây một lần, sau khi không được nhận vào hoạt động, không phải kích hoạt nữa để tự động kết nối lại với các PF hoặc WDH mà nó đã được nhận vào hoạt động. Giao tiếp Wi-Fi giữa WD và WDH mà nó được nhận vào hoạt động được bảo vệ sự riêng tư và toàn vẹn. Cũng các WD khác mà trước đó có thể đã được nhận vào hoạt động với WDH đó không thể giải mã truyền thông này hoặc làm xáo trộn nó mà không bị phát hiện. Tuyền thông Wi-Fi giữa WD và PF mà nó được kết nối trực tiếp đến trong khi nhận vào hoạt động được bảo vệ sự riêng tư và toàn vẹn. WD khác mà có thể trước đây đã được kết nối với các PF không thể giải mã cuộc truyền thông này hoặc làm xáo trộn nó mà không bị phát hiện. Truyền thông giữa WDH và PF kết nối Wi-Fi được bảo vệ sự riêng tư và tính toàn vẹn. WD không thể giải mã cuộc truyền thông này hoặc làm xáo trộn nó mà không bị phát hiện, mặc dù WD được nhận vào hoạt động với WDH này sẽ nhận được một số trong số các cuộc truyền thông này từ WDH và một số trong số các cuộc truyền thông này có nguồn gốc từ WD mà được nhận vào hoạt động với WDH này. WD mà được phép nhận vào hoạt động nhiều hơn một lần phải thực hiện WSC chỉ một lần khi nó nhận vào hoạt động lần thứ nhất và có thể được nhận vào hoạt động mà không sử dụng WSC khi được nhận vào hoạt động một lần nữa. WD và WDH cả hai có thể được cấu hình trước sao cho WD luôn có thể được nhận vào hoạt động tự động.

Trong hệ thống nhận vào hoạt động không dây tăng cường, các giai đoạn sau đây được định nghĩa: giai đoạn thiết lập (hoặc cấu hình), chế độ thôi không nhận vào hoạt

động, giai đoạn nhận vào hoạt động, và giai đoạn không nhận vào hoạt động, hoặc được kiểm soát hoặc không được kiểm soát.

Trong giai đoạn thiết lập, WDH thiết lập chính nó như là một P2P GO cho nhóm P2P G1 với SSID SSID1 và mật khẩu PP1. WDH chỉ chấp nhận PF cho tham gia Gl. Một số PF tham gia Gl sử dụng PBC hoặc WSC-PIN cho việc thu tnhận PP1. Các PF cũng có thể được cấu hình sẵn cho SSID1 và PP1.

Trong chế độ không được nhận vào hoạt động, WDH thiết lập chính nó như là một GO P2P cho nhóm P2P G2 với SSID SSID2 nhưng *không quyết định mật khẩu nào cho G2.* WDH có thể gửi các khung Beacon (báo trước) cho G2. WDH trả lời khung yêu cầu thăm dò. WDH cung cấp thông tin mà nó là WDH, trên PF của nó, trên WDE của nó, v.v. trong phần tử thông tin có liên quan. WDH chỉ chấp nhận WD cho gia nhập G2.

Trong giai đoạn nhận vào hoạt động, WD mà đã phát hiện G2 yêu cầu tham gia G2. Điều này gây nên hành động nhận vào hoạt động. Nếu WD không được phép nhận vào hoạt động, hành động nhận vào hoạt động được yêu cầu bị từ chối. Nếu WD đã được nhận vào hoạt động trước và nếu WD được phép nhận vào hoạt động một lần nữa, WDH đặt mật khẩu PP2 cho G2, mật khẩu mà nó đã sử dụng trước với WD đó. Trong tất cả các trường hợp khác (vì vậy khi WD đã không bao giờ được nhận vào hoạt động trước đó, hoặc khi nó đã được nhận vào hoạt động trước đó nhưng đã được phép nhận vào hoạt động chỉ một lần), WDH tạo ra PP2 ngẫu nhiên là mật khẩu cho G2. WDH gửi SSID2, PP2, địa chỉ WD và WD ID cho tất cả PF sử dụng nhóm P2P G1 (để được mã hóa bằng khóa được tạo ra từ PP1 và do đó được giữ riêng cho tất cả WD và tất cả các thiết bị khác). Nếu WD được cấu hình sẵn với mật khẩu cho WDH này hay vẫn sở hữu một mật khẩu từ phiên nhận vào hoạt động trước đó, nó có thể thử và sử dụng mật khẩu đó trong khi bắt tay bốn bên. Nếu không, hoặc khi sử dụng mật khẩu cũ không thành công, WD thực hiện WSC cho nhóm P2P G2 với WDH để thu nhận PP2. WSC có thể sử dụng PBS, hoặc WSC-PIN sử dụng hoặc là WD hoặc WDH PIN.

Nếu sau khi gia nhập G2, không PF nào được kết nối trực tiếp đến WDH, WD và WDH thiết lập kết nối tải qua WDH đến PF và WD được nhận vào hoạt động.

Nếu một hoặc nhiều PF sẽ được kết nối trực tiếp với WD, WD trao đổi vai trò GO với WDH. WDH gửi các địa chỉ/ID của tất cả PF hỗ trợ thiết lập kết nối Wi-Fi trực tiếp đến WD. Có thể loại trừ các địa chỉ của PF mà kết nối tải tốt nhất là được định tuyến qua WDH vì một số lý do. Chúng được gọi là PF 'trực tiếp'. Tất cả các PF khác được gọi là

PF 'gián tiếp'. Sử dụng nhóm P2P G1 như là phương tiện truyền thông, WDH yêu cầu PF trực tiếp tham gia nhóm P2P G2 sử dụng mật khẩu PP2. Hiệu quả trong ví dụ này là dữ liệu bí mật thứ hai giống dữ liệu bí mật thứ ba. Do PF trực tiếp biết PP2, chúng không cần phải thực hiện WSC để tham gia G2, điều này tiết kiệm thời gian đáng kể, thậm chí nếu như PIN được cung cấp trước. Các PF này chỉ cần thực hiện bắt tay bốn bên với WD sử dụng mật khẩu mà chúng biết (PP2). WD đã thu được địa chỉ của các PF trực tiếp liên quan đến sẽ biết mong đợi cho kết nối nào. Cả WD, qua G2, lẫn PF, qua Gl, có thể báo hiệu cho WDH rằng nhóm P2P G2 tham gia đã thành công hay thất bại. PF có thể không tham gia nhóm P2P G2 ví dụ như nếu khoảng cách giữa các PF và WD quá lớn. Các PF trực tiếp mà tham gia mà thất bại trở thành PF gián tiếp và duy trì kết nối với WDH. WD thiết lập kết nối tải trực tiếp cho PF đã gia nhập G2 thành công (tức là PF trực tiếp). kết nối tải được bảo vệ bằng cách sử dụng khóa được tạo ra từ PP2. WD và WDH thiết lập kết nối tải thông qua WDH đến các PF khác (tức là PF gián tiếp), và WD được nhận vào hoạt động. Nếu WDH hỗ trợ nhiều WD đồng thời, nó có thể thiết lập SSID mới để chấp nhận WD mới cho việc nhận vào hoạt động.

Trong pha không nhận vào hoạt động, việc không nhận vào hoạt động có thể được thực hiện theo cách có kiểm soát hoặc không kiểm soát. Việc nhận vào hoạt động có kiểm soát là nhờ đó mà WD chỉ rõ cho WDH rằng nó muốn không được nhận vào hoạt động. Việc không nhận vào hoạt động không kiểm soát được là khi WDH phát hiện ra bằng cách nào đó mà WD đã rời đi hoặc trở nên không thể truy cập mà không cần phải nhận được chỉ báo từ WD rằng nó muốn không được nhận vào hoạt động.

Trong khi không nhận vào hoạt động có kiểm soát, khi WD muốn không được nhận vào hoạt động, nó sẽ gửi cho WDH tin nhắn sử dụng nhóm P2P G2 như là phương tiện truyền thông mà nó muốn không nhận vào hoạt động. WDH báo nhận việc tiếp nhận thành công thông điệp này. Sau khi phân phối thành công tin nhắn đó, WD sẽ kết thúc phiên nhóm P2P G2 bằng cách gửi cho WDH và PF trong khung giải quyền G2 với lý do mã 3. Khi tiếp nhận khung giải quyền, PF phá bỏ kết nối tải. Sử dụng nhóm P2P Gl như là phương tiện truyền thông, WDH chỉ thị cho PF trực tiếp để xóa PP2 đã sử dụng. Ngoài ra, nó chỉ có thể làm điều này nếu WD không được phép nhận vào hoạt động một lần nữa. Trong trường hợp này, các PF có để lưu trữ mật khẩu và kết hợp WD ID để sử dụng sau này cho WD mà được phép nhận vào hoạt động một lần nữa. Điều này có thể tiết kiệm được khá nhiều thời gian của hoạt động nhận vào hoạt động. WDH phải theo dõi

việc PF đã nhận mật khẩu nào. WDH chỉ thị cho PF gián tiếp phá bỏ kết nối tải. WDH đảm nhiệm vai trò GO của nhóm P2P G2 và đặt mật khẩu là không được quyết định. Bây giờ WDH có thể quảng cáo về tình trạng không được nhận vào hoạt động một lần nữa.

Trong khi không nhận vào hoạt động không kiểm soát, WDH bằng cách nào đó quyết định rằng WD đã rời đi hoặc trở nên không thể truy cập mà không nhận được chỉ báo từ WD mà nó muốn không nhận vào hoạt động. WDH thông báo cho tất cả các PF phá bỏ kết nối tải (trực tiếp hoặc gián tiếp). Sử dụng nhóm P2P Gl như là phương tiện truyền thông, WDH chỉ thị cho các PF trực tiếp xóa PP2 dã sử dụng. Ngoài ra, nó chỉ có thể làm điều này nếu WD không được phép nhận vào hoạt động một lần nữa. Trong trường hợp này, các PF có để lưu trữ mật khẩu và kết hợp WD ID để sử dụng sau này cho WD mà được phép nhận vào hoạt động một lần nữa. Điều này có thể tiết kiệm được khá nhiều thời gian của hoạt động nhận vào hoạt động. WDH phải theo dõi việc PF đã nhận mật khẩu nào. Các WDH đảm nhiệm vai trò GO của nhóm P2P G2 và đặt mật khẩu là không được quyết định. Khi đó, WDH có thể quảng cáo về tình trạng không được nhận vào hoạt động một lần nữa.

Mặc dù sáng chế đã được mô tả qua các phương án sử dụng việc nhận vào hoạt động không dây, sáng chế cũng thích hợp cho bất kỳ hệ thống không dây nào trong đó thiết bị không dây chưa được kết nối cần được kết nối với nhóm thiết bị. Giải pháp của sáng chế liên quan đến việc nhận vào hoạt động thiết bị có khả năng Wi-Fi, thiết bị Serial Bus Wi-Fi, thiết bị hiển thị Wi-Fi, và thiết bị bất kỳ hỗ trợ Wi-Fi Direct khác nhau, từ thiết bị âm thanh mang được, điện thoại di động, máy tính xách tay, máy tính bảng đến chuột Wi-Fi, bàn phím, thiết bị hiển thị, máy in, máy ảnh.

Cũng cần lưu ý rằng giải pháp của sáng chế có thể được thực hiện bằng phần cứng và/hoặc phần mềm, sử dụng các thành phần có thể lập trình. Phương pháp thực hiện sáng chế có các bước tương ứng với chức năng được xác định cho hệ thống được mô tả dựa trên Fig.1.

Cần phải hiểu rằng phần mô tả trên đây, để rõ ràng, đã mô tả các phương án của sáng chế cho các bộ phận chức năng và bộ xử lý khác nhau. Tuy nhiên, rõ ràng là việc phân phối chức năng bất kỳ phù hợp giữa các bộ phận chức năng hoặc bộ xử lý khác nhau có thể được sử dụng và vẫn thuộc phạm vi của sáng chế. Ví dụ, các chức năng được minh họa được thực hiện bởi các bộ phận riêng biệt, bộ xử lý hoặc bộ điều khiển có thể được thực hiện bởi bộ xử lý tương tự hoặc bộ điều khiển. Do đó, việc dẫn chiếu đến chức

năng cụ thể được đưa ra chỉ để tham khảo các phương tiện phù hợp với chức năng được mô tả chứ không phải là thể hiện cấu trúc vật lý hay lôgic cụ thể. Sáng chế có thể được thực hiện dưới bất kỳ hình thức thích hợp nào bao gồm cả phần cứng, phần mềm, phần sụn hoặc bất kỳ sự kết hợp nào của chúng.

Cần lưu ý rằng trong tài liệu này thuật ngữ "bao gồm" không loại trừ sự hiện diện của phần tử khác hoặc các bước khác ngoài các phần tử được liệt kê và thuật ngữ 'một' trước phần tử không loại trừ sự hiện diện của nhiều phần tử đó, và rằng bất kỳ dấu hiệu dẫn chiếu nào cũng không làm giới hạn phạm vi của sáng chế, và rằng sáng chế có thể được thực hiện bằng phương tiện phần cứng và phần mềm, và rằng một số 'phương tiện' hoặc 'đơn vị' có thể được thể hiện bởi cùng một mục của phần cứng hoặc phần mềm, và bộ xử lý có thể thực hiện đầy đủ chức năng của một hoặc nhiều đơn vị, có thể phối hợp với phần cứng. Hơn nữa, sáng chế không bị giới hạn ở các phương án được mô tả, và sáng chế bao gồm mỗi và mọi dấu hiệu mới hoặc sự kết hợp các dấu hiệu được mô tả ở trên hoặc được thể hiện trong các điểm phụ thuộc.

YÊU CẦU BẢO HỘ

1. Hệ thống truyền thông không dây bao gồm nhóm thiết bị không dây (110, 120, 130, 140) và thiết bị mang được (200), mỗi thiết bị bao gồm bộ thu phát rađio để trao đổi dữ liệu với các thiết bị khác,

- thiết bị không dây thứ nhất của nhóm cung cấp chức năng máy chủ thứ nhất và thiết bị không dây thứ hai của nhóm cung cấp chức năng máy chủ thứ hai, thiết bị không dây thứ nhất và thiết bị không dây thứ hai là cùng thiết bị không dây hoặc là các thiết bị không dây khác nhau;

- nhóm thiết bị không dây (110, 120, 130, 140) chia sẻ dữ liệu bí mật thứ nhất (240) và được tạo cấu hình để truyền thông không dây với thiết bị không dây thứ nhất (100) cung cấp chức năng máy chủ thứ nhất thông qua kết nối bảo mật thứ nhất tương ứng dựa trên dữ liệu bí mật thứ nhất (240);

thiết bị mang được (200) bao gồm bộ xử lý truyền thông thiết bị (202) để:

- thiết lập kết nối bảo mật thứ hai với thiết bị không dây thứ hai (210) cung cấp chức năng máy chủ thứ hai sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai (250) khác với dữ liệu bí mật thứ nhất (240),

- nhận lệnh thứ hai thông qua kết nối bảo mật thứ hai, và, theo lệnh thứ hai này,

- thiết lập kết nối bảo mật không dây trực tiếp tương ứng với ít nhất một thiết bị không dây (110, 120, 140) của nhóm bằng cách sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba (420), dữ liệu bí mật thứ ba khác với dữ liệu bí mật thứ nhất (240);

thiết bị không dây thứ hai (210) cung cấp chức năng máy chủ thứ hai bao gồm bộ xử lý truyền thông máy chủ (102) để:

- thiết lập kết nối bảo mật thứ hai với thiết bị mang được (200) bằng cách sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai (250),

- chuyển đến ít nhất một thiết bị không dây thông qua kết nối bảo mật thứ nhất lệnh thứ nhất để áp dụng dữ liệu bí mật thứ ba (420) được chuyển theo lệnh thứ nhất để thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được (200), và

- chuyển đến thiết bị mang được (200) thông qua kết nối bảo mật thứ hai (SC) lệnh thứ hai để áp dụng dữ liệu bí mật thứ ba (420) được chuyển theo lệnh thứ hai để thiết lập kết nối bảo mật không dây trực tiếp với ít nhất một thiết bị không dây dựa trên dữ liệu bí mật thứ ba (420);

ít nhất một thiết bị không dây bao gồm bộ xử lý truyền thông (112) để:

- nhận lệnh thứ nhất thông qua kết nối bảo mật thứ nhất, và, theo lệnh thứ nhất,

- thiết lập kết nối bảo mật không dây trực tiếp tương ứng với thiết bị mang được (200) bằng cách sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba (420).

2. Thiết bị mang được (200) cho truyền thông không dây để sử dụng trong hệ thống theo điểm 1, thiết bị này bao gồm bộ thu phát radio để trao đổi dữ liệu không dây với các thiết bị không dây khác,

thiết bị mang được (200) bao gồm bộ xử lý truyền thông thiết bị (202) để:

- thiết lập kết nối bảo mật thứ hai với thiết bị không dây thứ hai (210) cung cấp chức năng máy chủ thứ hai sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai (250) khác với dữ liệu bí mật thứ nhất (240);

- nhận lệnh thứ hai thông qua kết nối bảo mật thứ hai, và, theo lệnh thứ hai này,

- thiết lập kết nối bảo mật không dây trực tiếp tương ứng với ít nhất một thiết bị không dây (110, 120, 140) của nhóm các thiết bị không dây bằng cách sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba (420), dữ liệu bí mật thứ ba khác với dữ liệu bí mật thứ nhất (240), dữ liệu bí mật thứ ba được chuyển theo lệnh thứ hai.

3. Thiết bị theo điểm 2, trong đó bộ xử lý truyền thông thiết bị (202) còn được bố trí để:

- kiểm soát sự truyền thông qua các kết nối không dây trực tiếp đã nêu dưới dạng chủ nhóm; và/hoặc

- thiết lập các kết nối bảo mật không dây trực tiếp khác nhau tương ứng với thiết bị không dây tương ứng của các tập con khác nhau của nhóm thiết bị không dây tương ứng bằng cách sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba khác nhau tương ứng, và/hoặc

- tạo ra dữ liệu bí mật thứ ba và chuyển dữ liệu bí mật thứ ba đến thiết bị cung cấp chức năng máy chủ thứ hai.

4. Thiết bị theo điểm 2, trong đó bộ xử lý truyền thông thiết bị (202) được bố trí để:

- ngắt kết nối bảo mật thứ hai trước khi bắt đầu thiết lập kết nối bảo mật không dây trực tiếp tương ứng với ít nhất một thiết bị không dây; và/hoặc

- cung cấp nhóm vĩnh cửu, và do đó, sau khi ngắt kết nối bảo mật không dây trực tiếp tương ứng dựa trên dữ liệu bí mật thứ ba (420), thiết lập kết nối bảo mật trực tiếp không dây tương ứng khác cũng dựa trên dữ liệu bí mật thứ ba (420), và/hoặc

- sử dụng dữ liệu bí mật thứ hai hoặc dữ liệu bí mật thứ ba thu được trong thời gian ghép cặp trước đó, sau khi ngắt kết nối bảo mật không dây trực tiếp tương ứng dựa trên dữ liệu bí mật thứ ba (420), kết nối lại với ít nhất một thiết bị không dây để thiết lập kết nối bảo mật không dây trực tiếp tương ứng.

5. Thiết bị theo điểm 2, trong đó:

- kết nối bảo mật thứ hai bao gồm kết nối Wi-Fi Direct P2P (kết nối không dây trực tiếp ngang hàng), và/hoặc

- kết nối bảo mật không dây trực tiếp tương ứng bao gồm kết nối Wi-Fi Direct P2P, hoặc

- kết nối bảo mật không dây trực tiếp tương ứng bao gồm kết nối thiết lập liên kết trực tiếp được tạo đường truyền (TDLS), và/hoặc

- thủ tục ghép cặp gồm thủ tục truy cập Wi-Fi được bảo vệ hoặc thủ tục cấu hình đơn giản Wi-Fi.

6. Thiết bị máy chủ cho truyền thông không dây để sử dụng trong hệ thống theo điểm 1, thiết bị này bao gồm:

bộ xử lý truyền thông máy chủ (102) để cung cấp chức năng máy chủ thứ hai, và

bộ thu phát radio không dây để trao đổi dữ liệu với thiết bị không dây khác bằng cách:

- thiết lập kết nối bảo mật thứ hai với thiết bị mang được (200) bằng cách sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai (250),

- chuyển cho ít nhất một thiết bị không dây thông qua kết nối bảo mật thứ nhất lệnh thứ nhất để áp dụng dữ liệu bí mật thứ ba (420) được chuyển theo lệnh thứ nhất để thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được (200), và

- chuyển đến thiết bị mang được (200) thông qua kết nối bảo mật thứ hai lệnh thứ hai để áp dụng dữ liệu bí mật thứ ba (420) được chuyển theo lệnh thứ hai để thiết lập kết nối bảo mật không dây trực tiếp với ít nhất một thiết bị không dây dựa trên dữ liệu bí mật thứ ba (420).

7. Thiết bị máy chủ theo điểm 6, trong đó bộ xử lý truyền thông máy chủ (102) được bố trí để:

- tạo ra dữ liệu bí mật thứ ba, và/hoặc

- tạo ra tập khác nhau tương ứng của dữ liệu bí mật thứ ba cho các thể hiện khác nhau tương ứng của thiết bị mang được (200), và/hoặc

- tạo ra tập khác nhau tương ứng của dữ liệu bí mật thứ ba khi thiết bị mang được (200), sau khi đã ngắt kết nối bảo mật thứ hai, đang thiết lập kết nối bảo mật thứ hai một thời gian thêm tương ứng, và/hoặc

- tạo ra tập khác nhau tương ứng của dữ liệu bí mật thứ ba cho tập con khác nhau tương ứng của thiết bị không dây, và/hoặc

- tạo ra dữ liệu bí mật thứ ba dựa trên, hoặc bằng với, dữ liệu bí mật thứ hai.

8. Thiết bị máy chủ theo điểm 6, trong đó bộ xử lý truyền thông máy chủ (102) được bố trí để:

- gán tuổi đời hạn chế cho dữ liệu bí mật thứ ba, và/hoặc

- gán tuổi đời cho dữ liệu bí mật thứ ba tùy thuộc vào mức quyền hoạt động của thiết bị (200).

9. Thiết bị máy chủ theo điểm 6, trong đó bộ xử lý truyền thông máy chủ (102) được bố trí để:

- chuyển lệnh thứ ba đến ít nhất một thiết bị không dây để ngắt kết nối kết nối bảo mật thứ nhất trước khi thiết lập kết nối bảo mật không dây trực tiếp tương ứng cho thiết bị mang được (200).

10. Thiết bị máy chủ theo điểm 6, trong đó thiết bị máy chủ là máy chủ nhận vào hoạt động không dây hoặc trạm nhận vào hoạt động không dây.

11. Thiết bị không dây (110) cho truyền thông không dây để sử dụng trong hệ thống theo điểm 1, hệ thống này bao gồm thiết bị mang được (200) và thiết bị không dây thứ nhất thuộc nhóm các thiết bị không dây, thiết bị không dây thứ nhất này cung cấp chức năng máy chủ thứ nhất và thiết bị không dây thứ hai thuộc nhóm cung cấp chức năng máy chủ thứ hai, thiết bị không dây thứ nhất và thiết bị không dây thứ hai là cùng một loại thiết bị không dây hoặc là các thiết bị không dây khác nhau,
thiết bị không dây này bao gồm:

bộ thu phát rađio để trao đổi dữ liệu với thiết bị mang được và các thiết bị không dây thứ nhất và thứ hai, và

bộ xử lý truyền thông (112) để:

- nhận lệnh thứ nhất thông qua kết nối bảo mật thứ nhất với thiết bị không dây thứ nhất, và, theo lệnh thứ nhất này,

- thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được (200) bằng cách sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ ba (420), dữ liệu bí mật thứ ba này khác dữ liệu bí mật thứ nhất (240) trên đó kết nối bảo mật thứ nhất dựa trên, dữ liệu bí mật thứ ba được nhận bằng lệnh thứ nhất.

12. Thiết bị không dây theo điểm 11, trong đó bộ xử lý truyền thông (112) được bố trí để

- khởi tạo việc thành lập kết nối bảo mật không dây trực tiếp cho thiết bị mang được (200).

13. Thiết bị không dây theo điểm 11, trong đó bộ xử lý truyền thông (112) được bố trí để:

- ngắt kết nối bảo mật thứ nhất trước khi thiết lập kết nối bảo mật không dây trực tiếp với thiết bị mang được (200), và/hoặc

- khôi phục kết nối bảo mật thứ nhất sau khi ngắt kết nối bảo mật không dây trực tiếp với thiết bị mang được (200).

14. Phương pháp truyền thông không dây trong hệ thống thiết bị không dây theo điểm 1, phương pháp này bao gồm các bước sau đây:

- thiết lập kết nối bảo mật thứ hai giữa thiết bị mang được (200) và thiết bị không dây thứ hai (210) cung cấp chức năng máy chủ thứ hai sử dụng thủ tục ghép cặp dựa trên dữ liệu bí mật thứ hai (250) khác với dữ liệu bí mật thứ nhất (240) mà kết nối thứ nhất với thiết bị không dây thứ nhất dựa trên đó;

- chuyển đến ít nhất một thiết bị không dây của nhóm các thiết bị không dây thông qua kết nối bảo mật thứ nhất lệnh thứ nhất áp dụng dữ liệu bí mật thứ ba (420) được chuyển theo lệnh thứ nhất để thiết lập kết nối bảo mật trực tiếp không dây với thiết bị mang được (200), dữ liệu bí mật thứ ba khác với dữ liệu bí mật thứ nhất (240), và

- chuyển đến thiết bị mang được (200) thông qua kết nối bảo mật thứ hai lệnh thứ hai để áp dụng dữ liệu bí mật thứ ba (420) được chuyển theo lệnh thứ hai để thiết lập kết nối bảo mật không dây trực tiếp với ít nhất một thiết bị không dây dựa trên dữ liệu bí mật thứ ba (420);

- thiết lập kết nối bảo mật không dây trực tiếp tương ứng giữa thiết bị mang được và ít nhất một thiết bị không dây sử dụng thủ tục ghép cặp tương ứng dựa trên dữ liệu bí mật thứ ba (420).

15. Vật ghi đọc được bởi máy tính chứa mã lệnh mà khi được thực hiện bởi bộ xử lý của hệ thống theo điểm 1 sẽ khiến máy tính thực hiện các bước của phương pháp truyền thông theo điểm 14.

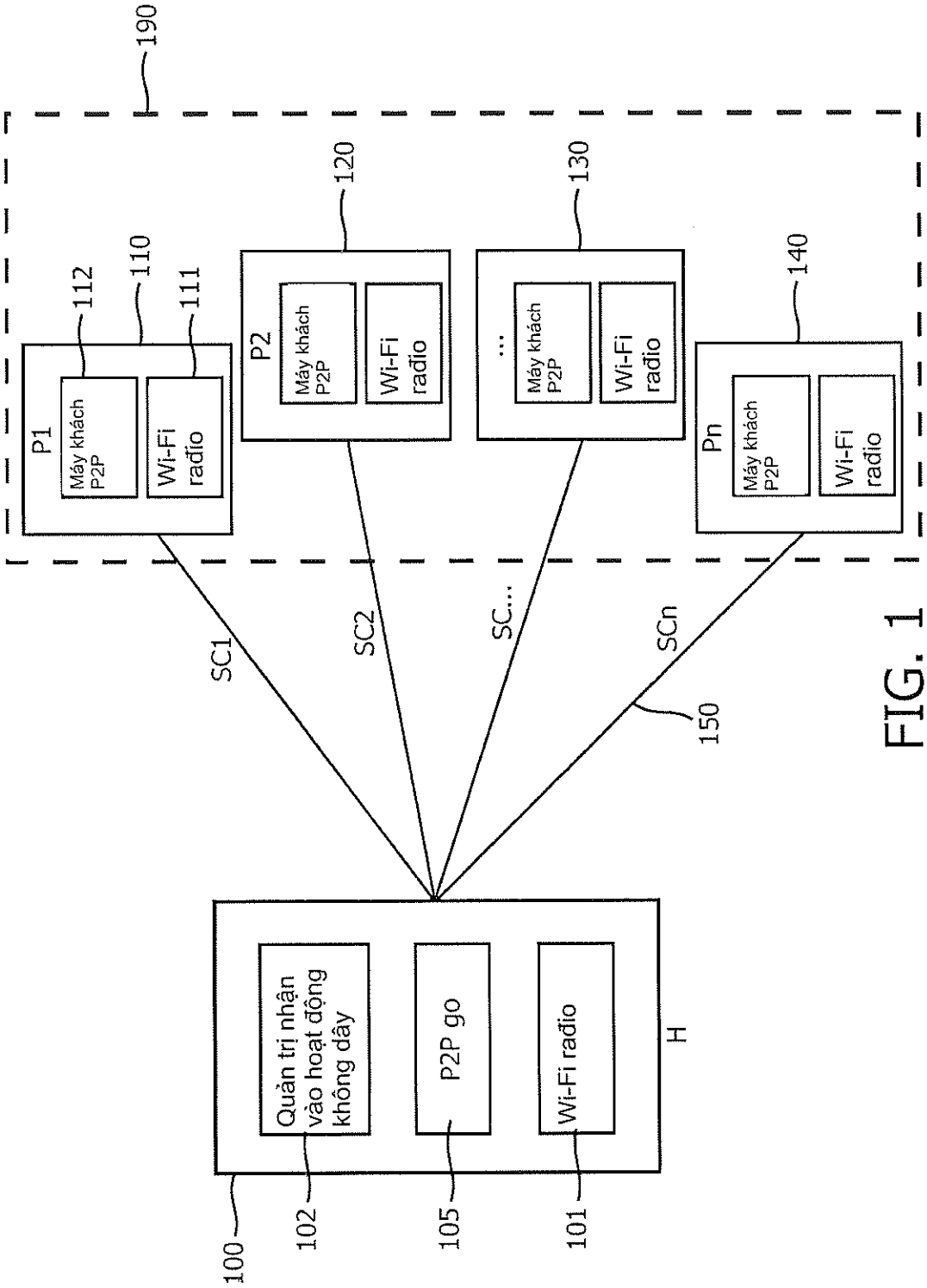

190
P1
Máy khách P2P
Wi-Fi radio
112
111
110
P2
Máy khách P2P
Wi-Fi radio
120
...
Máy khách P2P
Wi-Fi radio
130
Pn
Máy khách P2P
Wi-Fi radio
140
SC1
SC2
SC...
SCn
150
H
Quản trị nhận vào hoạt động không dây
P2P go
Wi-Fi radio
100
102
105
101

FIG. 1

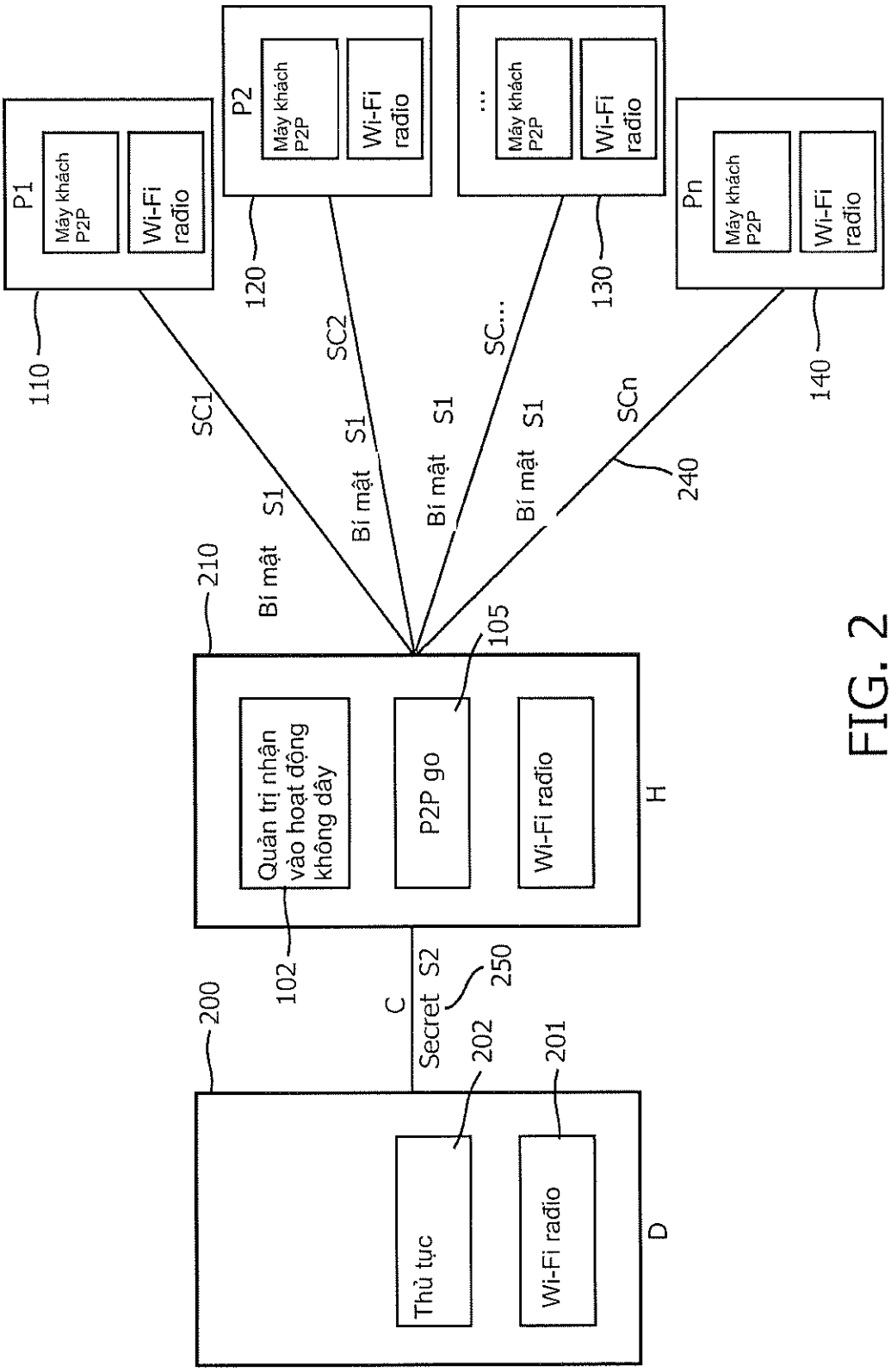

P1
Máy khách P2P
Wi-Fi radio
110
P2
Máy khách P2P
Wi-Fi radio
120
...
Máy khách P2P
Wi-Fi radio
130
Pn
Máy khách P2P
Wi-Fi radio
140
SC1
SC2
SC...
SCn
S1
Bí mật
240
210
105
Quản trị nhận vào hoạt động không dây
P2P go
Wi-Fi radio
H
102
C
Secret
S2
250
200
202
201
Thủ tục
Wi-Fi radio
D

FIG. 2

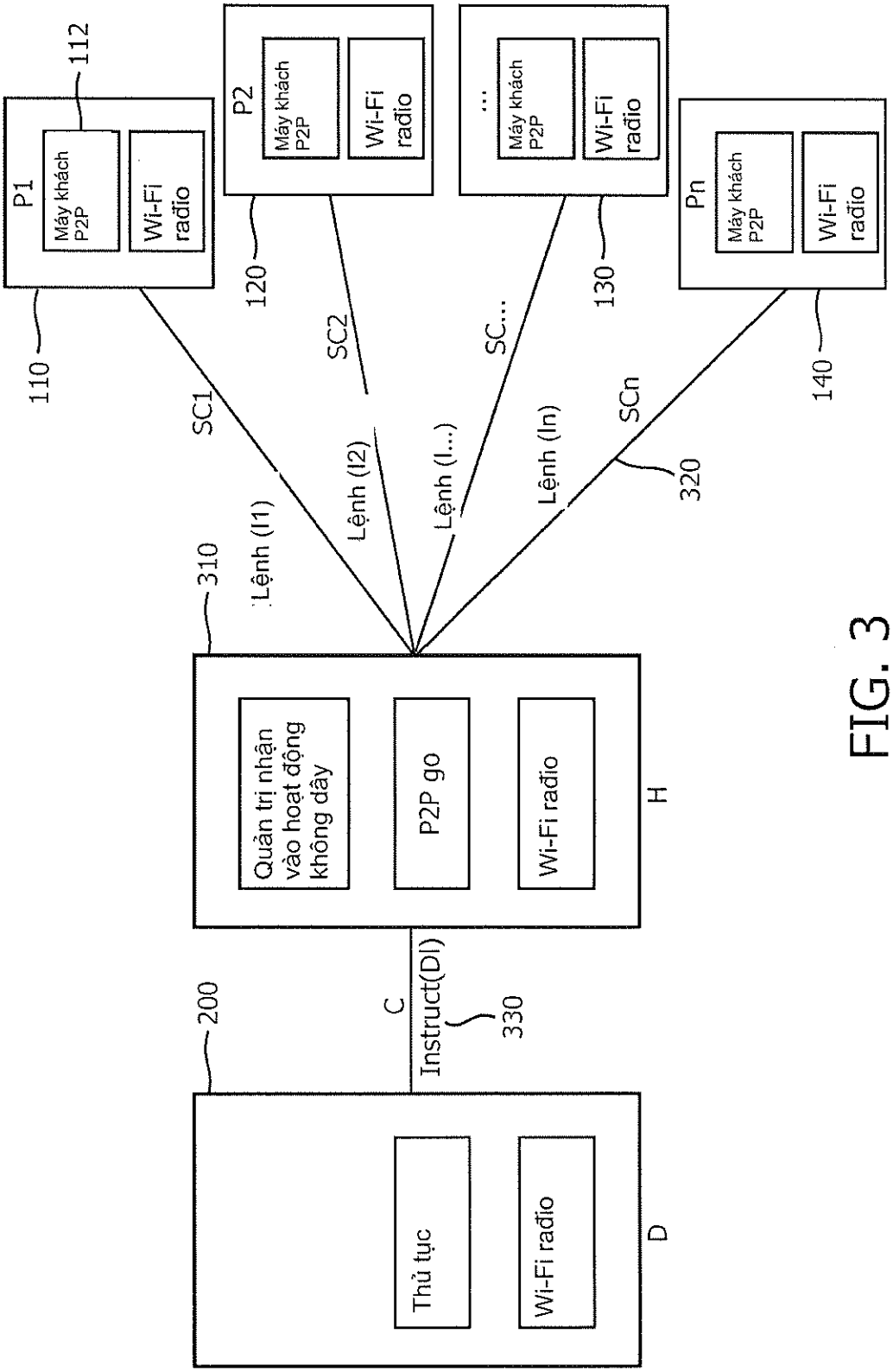

P1
Máy khách P2P
Wi-Fi radio
112
110
P2
Máy khách P2P
Wi-Fi radio
120
...
Máy khách P2P
Wi-Fi radio
130
Pn
Máy khách P2P
Wi-Fi radio
140
SC1
SC2
SC...
SCn
Lệnh (I1)
Lệnh (I2)
Lệnh (I...)
Lệnh (In)
320
310
Quản trị nhận vào hoạt động không dây
P2P go
Wi-Fi radio
H
C
Instruct(DI)
330
200
Thủ tục
Wi-Fi radio
D

FIG. 3

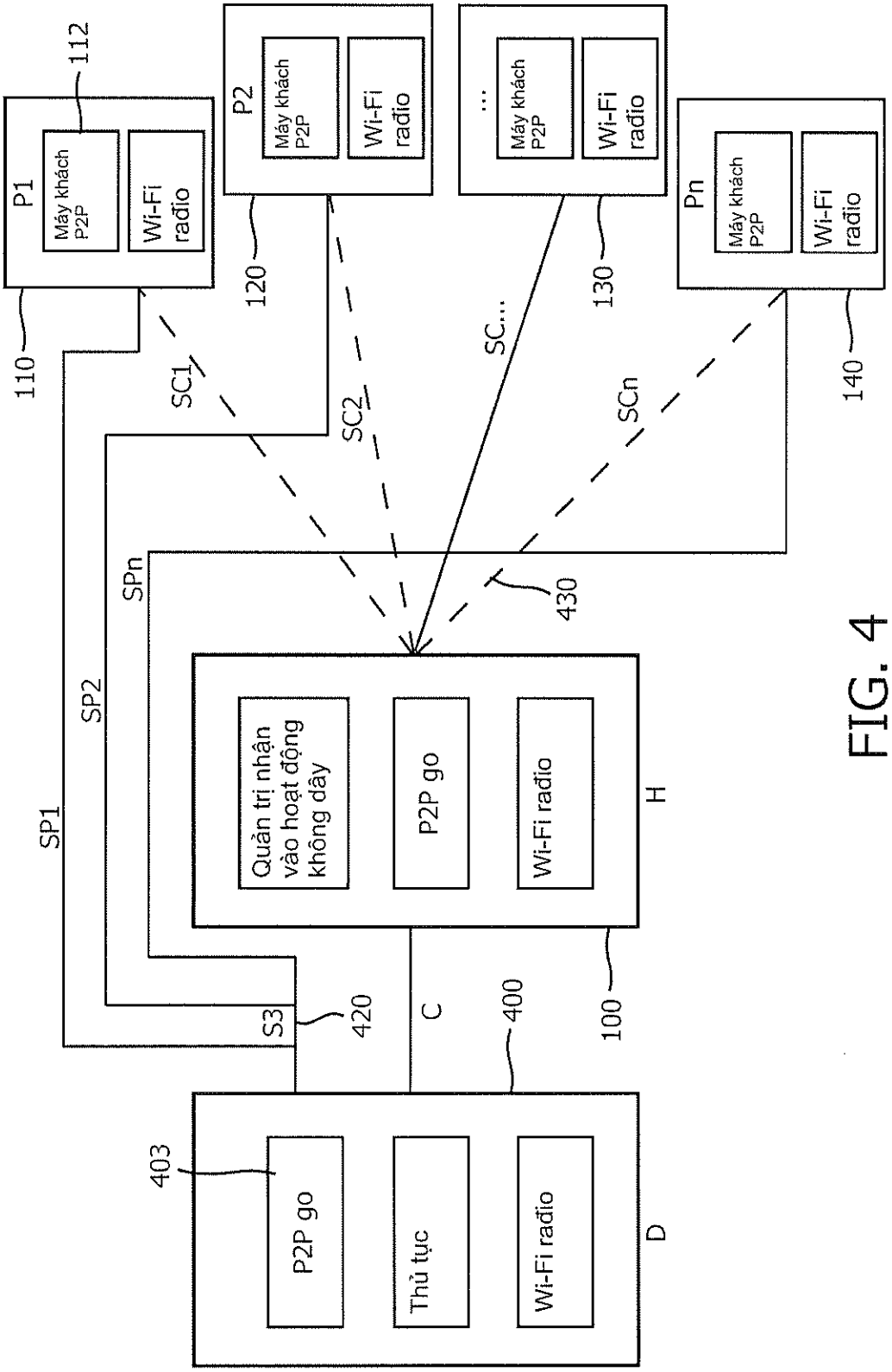

P1
Máy khách P2P
Wi-Fi radio
112
110
P2
Máy khách P2P
Wi-Fi radio
120
...
Máy khách P2P
Wi-Fi radio
130
Pn
Máy khách P2P
Wi-Fi radio
140
SC1
SC2
SC...
SCn
SP1
SP2
SPn
430
Quản trị nhận vào hoạt động không dây
P2P go
Wi-Fi radio
H
S3
420
C
400
100
403
P2P go
Thủ tục
Wi-Fi radio
D

FIG. 4