(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) **1-0047821**

(51)[2021.01] **H04L 12/24**; H04W 12/00; H04L 29/06 (13) **B**

(21) 1-2022-04466 (22) 18/12/2019
(86) PCT/EP2019/085893 18/12/2019 (87) WO 2021/121574 24/06/2021
(45) 25/06/2025 447 (43) 26/09/2022 414A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building Bantian, Longgang District Shenzhen, Guangdong 518129, China
(72) POGORELIK, Oleg (IL).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP THỰC HIỆN THƯƠNG LƯỢNG BẢO MẬT CHO CẤU HÌNH MẠNG, THIẾT BỊ MẠNG, THIẾT BỊ TRUYỀN THÔNG VÀ VẬT GHI MÁY TÍNH ĐỌC ĐƯỢC

(21) 1-2022-04466

(57) Sáng chế đề cập đến phương pháp thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị mạng, bao gồm thu được, bởi thiết bị mạng, thông tin cập nhật bảo mật từ thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất. Bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Phương pháp còn bao gồm xác định, bởi thiết bị mạng, bộ phận bảo mật thứ hai đối với thiết bị truyền thông dựa trên thông tin cập nhật bảo mật. Lệnh được cấp bởi thiết bị mạng cho thiết bị truyền thông để gia nhập bộ phận bảo mật thứ hai được xác định.

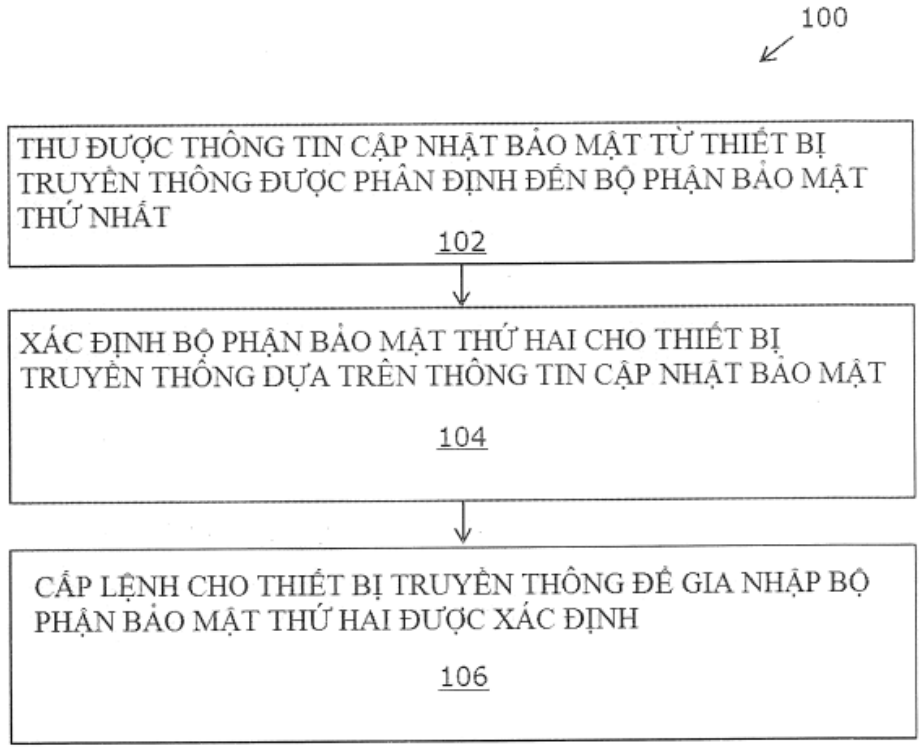

Fig.1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập chung đến lĩnh vực quản lý và bảo mật mạng; và cụ thể hơn, đến phương pháp và thiết bị thực hiện thương lượng bảo mật cho cấu hình mạng.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển nhanh của hạ tầng mạng, các quan ngại về quản lý và bảo mật mạng trở nên nổi bật. Hiện tại, phân đoạn mạng được sử dụng rộng rãi để quản lý các rủi ro của các lỗ hổng bảo mật. Thông thường, các bộ phận mạng là các đoạn của mạng được tách khỏi các bộ phận khác nhờ sử dụng thiết bị mạng đã biết (chẳng hạn, thiết bị cổng nối, bộ định tuyến, và tương tự). Các thiết bị truyền thông khác nhau (chẳng hạn, máy tính xách tay, thiết bị IoT, điện thoại thông minh, máy chủ, và tương tự) thường được tạo nhóm có chọn lọc thành các bộ phận mạng khác nhau để quản lý các rủi ro của các lỗ hổng bảo mật trong các thiết bị truyền thông được nối với mạng cũng như hạ tầng mạng. Trong các phương pháp và hệ thống đã biết, các quyết định liên quan đến việc liên kết bộ phận mạng được thực hiện dựa trên giả thiết rằng thiết bị mạng đã biết nhận thức và điều khiển tất cả các chức năng và các hoạt động liên quan đến mạng. Do vậy, các quyết định liên quan đến việc liên kết bộ phận mạng được xem xét toàn bộ bởi thiết bị mạng, vốn không mong muốn. Chẳng hạn, thiết bị mạng đã biết có thể không phân định bộ phận mạng cụ thể (hoặc phân định bộ phận mạng không phù hợp) cho thiết bị mạng cụ thể, vốn chưa được biết (chẳng hạn, loại thiết bị không hỗ trợ) và minh họa hành vi mạng không dự báo được. Việc không phân định bất kỳ bộ phận mạng cụ thể hoặc phân định bộ phận mạng không thích hợp (tức là, không so khớp bộ phận) có thể đặt ra rủi ro bảo mật. Trong ví dụ khác, thiết bị truyền thông (chẳng hạn, bộ điều khiển IoT) có thể truyền thông với các thiết bị truyền thông ngang hàng (chẳng hạn, các

thiết bị IoT khác) và máy chủ đám mây qua mạng tùy chọn (chẳng hạn, mạng tế bào) bỏ qua kênh truyền thông thông thường (chẳng hạn, mạng Wi-Fi) với thiết bị mạng đã biết. Do vậy, phiên truyền thông này qua mạng tùy chọn có thể không khả dụng (tức là, vô hình) với thiết bị mạng đã biết qua kênh truyền thông thông thường. Trong các trường hợp này, thiết bị mạng đã biết không thể nhận thức tất cả các chức năng và hoạt động mạng liên quan, và do vậy không thể thực hiện đầy đủ cấu hình mạng, dẫn đến thỏa hiệp trong bảo mật mạng (tức là, khe bảo mật). Nói cách khác, trong các trường hợp này, cấu hình và liên kết mạng động của bộ phận mạng với thiết bị truyền thông đã biết bằng thiết bị mạng đã biết có thể gặp phải nhiều thách thức kỹ thuật, chẳng hạn sai khớp bộ phận mạng và bảo mật không đầy đủ. Ngoài ra, trong các trường hợp này, các thiết bị truyền thông đã biết có thể không hoạt động phù hợp và có thể yêu cầu nhiều công sức thủ công ở thiết bị mạng đã biết để quản lý và cấu hình mạng.

Do vậy, theo mô tả nêu trên, cần khắc phục các nhược điểm nêu trên được liên kết với các phương pháp, các hệ thống, và các thiết bị đã biết để quản lý và bảo mật mạng.

Bản chất kỹ thuật của sáng chế

Sáng chế đề cập đến phương pháp, thiết bị, và sản phẩm chương trình máy tính thực hiện thương lượng bảo mật cho cấu hình mạng. Sáng chế đề cập đến giải pháp cho vấn đề hiện tại quản lý mạng và bảo mật mạng không đủ như là kết quả của các quyết định liên quan đến liên kết bộ phận mạng được xem xét toàn bộ bởi thiết bị mạng đã biết. Mục đích của sáng chế là đề cập đến giải pháp khắc phục ít nhất một phần vấn đề gặp phải theo giải pháp kỹ thuật đã biết, và đề xuất các phương pháp và thiết bị cải thiện có thể quản lý mạng hiệu quả và cung cấp đầy đủ bảo mật mạng.

Mục đích của sáng chế đạt được bởi các giải pháp theo các điểm yêu cầu bảo hộ độc lập đi kèm. Các cách thức thực hiện có lợi của sáng chế còn được định nghĩa trong các điểm yêu cầu bảo hộ phụ thuộc.

Theo khía cạnh thứ nhất, sáng chế provides phương pháp thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị mạng. Phương pháp bao gồm các

bước thu được, bởi thiết bị mạng, thông tin cập nhật bảo mật từ thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất. Bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Phương pháp còn bao gồm bước xác định, bởi thiết bị mạng, bộ phận bảo mật thứ hai đối với thiết bị truyền thông dựa trên thông tin cập nhật bảo mật. Phương pháp còn bao gồm bước cấp, bởi thiết bị mạng, lệnh cho thiết bị truyền thông để gia nhập bộ phận bảo mật thứ hai được xác định.

Phương pháp theo khía cạnh thứ nhất khiến thiết bị mạng có thể xác định bộ phận bảo mật thích hợp (tức là, bộ phận mạng đúng) từ các bộ phận bảo mật thực hiện thay đổi mới nhất trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Do thông tin cập nhật bảo mật thu được từ thiết bị truyền thông được sử dụng khi xác định bộ phận bảo mật thứ hai bởi thiết bị mạng, các cơ hội sai khớp bộ phận bảo mật được giảm đáng kể, nhờ đó giảm rủi ro của các lỗ hổng bảo mật trong thiết bị truyền thông và cải thiện toàn bộ bảo mật mạng. Ngoài ra, do các cơ hội sai khớp bộ phận bảo mật được giảm đáng kể, công sức thủ công quản lý và cấu hình mạng không được yêu cầu hoặc ít nhất bị giảm, nhờ đó cải thiện hiệu suất trong quản lý mạng.

Ở dạng thực hiện thứ nhất của khía cạnh thứ nhất, phương pháp còn bao gồm bước cấp, bởi thiết bị mạng, cho thiết bị truyền thông, tiểu sử bảo mật bộ phận thứ hai được liên kết với bộ phận bảo mật thứ hai được xác định. Tiểu sử bảo mật bộ phận thứ hai được sử dụng bởi thiết bị truyền thông để: kiểm chứng quyết định để gia nhập bộ phận bảo mật thứ hai; và điều khiển, dựa trên kiểm chứng, kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông theo tiểu sử bảo mật bộ phận thứ hai.

Tiểu sử bảo mật bộ phận thứ hai được chia sẻ với thiết bị truyền thông khiến thiết bị truyền thông có thể kiểm chứng quyết định liệu có gia nhập bộ phận bảo mật thứ hai hay không, và do vậy việc chủ động tham gia của thiết bị truyền thông được đảm bảo trong các quyết định liên quan đến liên kết với bộ phận bảo mật thứ hai được xác định. Trong các trường hợp trong đó kiểm chứng thành công, các chức năng hoặc các dịch vụ cụ thể ở thiết bị truyền

thông vốn đã trở nên không tương thích do thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông, được kích hoạt hoặc vô hiệu hóa (chẳng hạn, các chức năng không bảo mật có thể bị vô hiệu hóa) theo tiểu sử bảo mật bộ phận thứ hai.

Theo dạng triển khai thứ hai của khía cạnh thứ nhất, việc thu được thông tin cập nhật bảo mật bởi thiết bị mạng dựa trên thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hoặc thay đổi trong môi trường mạng của thiết bị truyền thông.

Thay đổi trong trạng thái hoạt động của thiết bị hoặc môi trường mạng của thiết bị truyền thông thay đổi động tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Do vậy, việc thu được thông tin cập nhật bảo mật chỉ báo (các) thay đổi này khiến thiết bị mạng có thể nhanh chóng đóng các khe hở bảo mật mà có thể phát sinh do các thay đổi này ở thiết bị truyền thông.

Theo dạng triển khai thứ ba của khía cạnh thứ nhất, việc xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông bao gồm bước so sánh các thuộc tính bảo mật được liên kết với ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất với các thuộc tính bảo mật tương ứng được liên kết với mỗi tiểu sử trong các tiểu sử bảo mật bộ phận được liên kết với các bộ phận bảo mật.

Việc so sánh các thuộc tính bảo mật đảm bảo rằng bộ phận bảo mật so khớp tốt nhất với thay đổi được chỉ báo giữa các bộ phận bảo mật được xác định đối với thiết bị truyền thông.

Theo dạng triển khai thứ tư của khía cạnh thứ nhất, phương pháp còn bao gồm áp dụng chính sách mạng cụ thể được liên kết với bộ phận bảo mật thứ hai đối với thiết bị truyền thông sau khi thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai và rời khỏi bộ phận bảo mật thứ nhất.

Ứng dụng của chính sách mạng cụ thể được liên kết với bộ phận bảo mật thứ hai cho phép bảo mật mạng đầy đủ và đảm bảo rằng truy nhập được cấp cho một hoặc nhiều dịch vụ mới được yêu cầu bởi thiết bị truyền thông như là kết quả của ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông sau khi thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai và

rời khỏi bộ phận bảo mật thứ nhất. Tương tự, các dịch vụ cụ thể không còn được yêu cầu bị vô hiệu hóa (chẳng hạn, truy nhập bị thu hồi) để thu nhỏ hoặc ít nhất giảm rủi ro của các lỗ hổng bảo mật trong thiết bị truyền thông được nối với mạng (chẳng hạn, mạng Internet) qua thiết bị mạng.

Theo dạng triển khai thứ năm của khía cạnh thứ nhất, tiểu sử bảo mật thứ nhất bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông, hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông. Tiểu sử bảo mật thứ nhất được cập nhật bởi thiết bị truyền thông thành tiểu sử bảo mật thứ hai dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hoặc thay đổi trong môi trường mạng của thiết bị truyền thông.

Tiểu sử bảo mật thứ nhất của thiết bị truyền thông động và không tĩnh, và do vậy bất kỳ thay đổi nào trong trạng thái hoạt động của thiết bị hoặc bất kỳ thay đổi trong môi trường mạng trong đó thiết bị truyền thông hoạt động, có thể được chứa đựng trong tiểu sử bảo mật thứ nhất. Do vậy, ngược với hệ thống và phương pháp đã biết, phương pháp có thể hỗ trợ các kịch bản trong đó tiểu sử bảo mật thiết bị (tức là, nội dung của tiểu sử bảo mật thứ nhất của thiết bị truyền thông) thay đổi đột ngột do thay đổi trong trạng thái hoạt động của thiết bị hoặc thay đổi trong môi trường mạng của thiết bị truyền thông.

Theo dạng triển khai thứ sáu của khía cạnh thứ nhất, thông tin cập nhật bảo mật tương ứng với ít nhất một trong: tiểu sử bảo mật thứ hai hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất. Tiểu sử bảo mật thứ hai bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông, yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ trong bộ phận bảo mật thứ nhất được phân định cho thiết bị truyền thông, hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông.

Thông tin cập nhật bảo mật khiến thiết bị mạng có thể nhận thức bất kỳ thay đổi trong các chức năng và các hoạt động liên quan đến mạng thậm chí

nếu bất kỳ truyền thông nào liên quan đến mạng bỏ qua kênh truyền thông thông thường với thiết bị mạng. Do vậy, phương pháp có thể đóng nhanh chóng và đầy đủ các khe hở bảo mật có thể tiềm tàng phát sinh do cập nhật hoặc thay đổi trong tiểu sử bảo mật thứ nhất (tức là, các yêu cầu bảo mật) của thiết bị truyền thông.

Ở dạng triển khai thứ bảy của khía cạnh thứ nhất, việc xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông bao gồm việc sử dụng bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ hai.

Bằng cách xem xét bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ hai, độ chính xác khi xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông được tăng lên, nhờ đó cải thiện hiệu suất trong quản lý mạng và giảm rủi ro bảo mật.

Theo dạng triển khai thứ tám của khía cạnh thứ nhất, thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất dựa trên hoạt động gia nhập lần đầu tiên giữa thiết bị mạng và thiết bị truyền thông. Hoạt động gia nhập lần đầu tiên bao gồm thu được, bởi thiết bị mạng, tiểu sử bảo mật thứ nhất từ thiết bị truyền thông theo bộ phận thương lượng khi thiết bị truyền thông ở trạng thái không được phân định đến bộ phận bảo mật cụ thể. Tiểu sử bảo mật thứ nhất chỉ báo các khả năng của thiết bị và các yêu cầu bảo mật của thiết bị truyền thông ở trạng thái không được phân định. Hoạt động gia nhập lần đầu tiên còn bao gồm xác định, bởi thiết bị mạng, bộ phận bảo mật thứ nhất từ các bộ phận bảo mật để phân định cho thiết bị truyền thông dựa trên tiểu sử bảo mật thứ nhất thu được. Hoạt động gia nhập lần đầu tiên còn bao gồm bước cấp, bởi thiết bị mạng, lệnh cho thiết bị truyền thông để gia nhập bộ phận bảo mật thứ nhất, trong đó lệnh thông báo thiết bị truyền thông của bộ phận bảo mật thứ nhất được xác định liên quan đến các khả năng thiết bị và các yêu cầu bảo mật của thiết bị truyền thông.

Tiểu sử bảo mật thứ nhất có thể đánh giá tăng cường các khả năng bảo mật và các yêu cầu bảo mật của thiết bị truyền thông bởi thiết bị mạng. Chẳng hạn, các đặc tính bảo mật cụ thể (hoặc thuộc tính bảo mật) của thiết bị truyền thông mà bên cạnh đó có thể vẫn chưa được dò thấy (tức là, chưa bị lộ) qua kênh

truyền thông thông thường (chẳng hạn, sử dụng chức năng tự phát hiện) bởi thiết bị mạng, được phát hiện dễ dàng và chính xác nhờ sử dụng tiểu sử bảo mật thứ nhất. Do vậy, tiểu sử bảo mật thứ nhất khiến thiết bị mạng có thể xác định bộ phận bảo mật so khớp tốt nhất (tức là, bộ phận bảo mật thứ nhất trong trường hợp này) từ trong số các bộ phận bảo mật để phân định cho thiết bị truyền thông, nhờ đó bảo mật đầy đủ.

Theo khía cạnh thứ hai, sáng chế đề cập đến phương pháp thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị truyền thông. Phương pháp bao gồm bước cấp, bởi thiết bị truyền thông, thông tin cập nhật bảo mật cho thiết bị mạng. Thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Phương pháp còn bao gồm bước thu được, bởi thiết bị truyền thông, lệnh từ thiết bị mạng để gia nhập bộ phận bảo mật thứ hai. Phương pháp còn bao gồm bước gia nhập, bởi thiết bị truyền thông, bộ phận bảo mật thứ hai thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông, dựa trên lệnh thu được.

Phương pháp có thể tham gia chủ động của thiết bị truyền thông cùng với thiết bị mạng trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật (chẳng hạn, bộ phận bảo mật thứ hai được xác định trong trường hợp này). Do thông tin cập nhật bảo mật được chủ động chia sẻ bởi thiết bị truyền thông, thiết bị mạng có thể xác định đúng bộ phận bảo mật (tức là, bộ phận bảo mật thứ hai trong trường hợp này) từ các bộ phận bảo mật thực hiện thay đổi mới nhất trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Do vậy, các cơ hội sai khớp bộ phận bảo mật được giảm đáng kể, nhờ đó giảm rủi ro của các lỗ hổng bảo mật trong thiết bị truyền thông và cải thiện toàn bộ bảo mật mạng và hiệu suất trong quản lý mạng. Việc gia nhập bộ phận bảo mật thứ hai bởi thiết bị truyền thông có thể đóng nhanh chóng và đầy đủ các khe hở bảo mật có thể tiềm tàng phát sinh do cập nhật hoặc thay đổi (chẳng hạn, các thay đổi trong các thuộc tính bảo mật, dịch vụ, hoặc thuộc tính cụ thể) trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông.

Ở dạng thực hiện thứ nhất theo khía cạnh thứ hai, thông tin cập nhật bảo mật được cấp bởi thiết bị truyền thông cho thiết bị mạng dựa trên thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hoặc thay đổi trong môi trường mạng của thiết bị truyền thông.

Thông tin cập nhật bảo mật chỉ báo (các) thay đổi này được chủ động cấp bởi thiết bị truyền thông cho thiết bị mạng sao cho thiết bị mạng có thể đóng nhanh chóng các khe hở bảo mật có thể tiềm tàng phát sinh do các thay đổi ở thiết bị truyền thông.

Ở dạng triển khai thứ hai theo khía cạnh thứ hai, tiểu sử bảo mật thứ nhất bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông, hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông.

Tiểu sử bảo mật thứ nhất là tổng hợp và xác định đầy đủ các khả năng của thiết bị và các yêu cầu bảo mật của thiết bị truyền thông. Chẳng hạn, loại thiết bị, danh sách truy nhập bộ định vị tài nguyên thống nhất (uniform resource locator, URL), các giao thức được hỗ trợ, các cổng đóng hoặc mở, các yêu cầu truy nhập các tài nguyên mạng cụ thể hoặc các dịch vụ hoặc vô hiệu hóa các dịch vụ khác cụ thể, tải xuống hoặc tải lên các cấp quyền, và tương tự, được xác định trong tiểu sử bảo mật thứ nhất. Do vậy, thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi (chẳng hạn, bất kỳ thay đổi trong các thuộc tính thiết bị, môi trường mạng, thay đổi trong yêu cầu truy nhập các dịch vụ mới hoặc vô hiệu hóa các dịch vụ đang được truy nhập) của tiểu sử bảo mật thứ nhất, khiến thiết bị mạng có thể xác định bộ phận so khớp tốt nhất từ các bộ phận bảo mật để thỏa mãn thay đổi mới nhất trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông.

Ở dạng triển khai thứ ba theo khía cạnh thứ hai, phương pháp còn bao gồm bước cập nhật, bởi thiết bị truyền thông, tiểu sử bảo mật thứ nhất thành tiểu sử bảo mật thứ hai dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hojặc thay đổi trong môi trường mạng của thiết bị truyền thông.

Tiểu sử bảo mật thứ nhất của thiết bị truyền thông là động và không tĩnh, và do vậy bất kỳ thay đổi trong trạng thái hoạt động của thiết bị hoặc bất kỳ thay đổi trong môi trường mạng trong đó thiết bị truyền thông hoạt động, có thể được chứa đựng trong tiểu sử bảo mật thứ nhất. Việc cập nhật tiểu sử bảo mật thứ nhất thành tiểu sử bảo mật thứ hai có thể ghi nhận thông tin gần đây nhất liên quan đến các thuộc tính thiết bị, bất kỳ thay đổi trong trạng thái hoạt động của thiết bị, hoặc bất kỳ thay đổi trong môi trường mạng của thiết bị truyền thông.

Ở dạng triển khai thứ tư theo khía cạnh thứ hai, thông tin cập nhật bảo mật tương ứng với ít nhất một trong: tiểu sử bảo mật thứ hai hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất, và trong đó tiểu sử bảo mật thứ hai bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông, yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ bởi bộ phận bảo mật thứ nhất, hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông, và trong đó bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ hai được sử dụng bởi thiết bị mạng để xác định bộ phận bảo mật thứ hai.

Thông tin cập nhật bảo mật khiến thiết bị mạng có thể nhận thức bất kỳ thay đổi nào trong các chức năng và các hoạt động liên quan đến mạng của thiết bị truyền thông thậm chí nếu truyền thông liên quan đến mạng bất kỳ bỏ qua kênh truyền thông thông thường với thiết bị mạng. Do vậy, phương pháp có thể đóng nhanh chóng và đầy đủ các khe hở bảo mật có thể tiềm tàng phát sinh do cập nhật hoặc thay đổi liên quan đến các yêu cầu bảo mật của thiết bị truyền thông.

Ở dạng triển khai thứ tư theo khía cạnh thứ hai, việc gia nhập bộ phận bảo mật thứ hai bao gồm thu được, bởi thiết bị truyền thông, từ thiết bị mạng, một hoặc nhiều trong số: danh sách dịch vụ bảo mật được hỗ trợ bởi thiết bị mạng cho bộ phận bảo mật thứ hai, tiểu sử bảo mật bộ phận thứ hai được liên kết với

bộ phận bảo mật thứ hai, hoặc các tiểu sử bảo mật bộ phận cho các bộ phận bảo mật khả dụng với thiết bị mạng.

Việc thu được thông tin này (chẳng hạn danh sách các dịch vụ bảo mật, tiểu sử bảo mật bộ phận thứ hai, và các tiểu sử bảo mật bộ phận khả dụng khác) có thể thương lượng bảo mật và kiểm chứng bảo mật lẫn nhau giữa thiết bị truyền thông và thiết bị mạng. Nói cách khác, cả thiết bị mạng và thiết bị truyền thông có thể thực thi thương lượng bảo mật để cho phép cả cấu hình mạng lần đầu và cấu hình mạng theo yêu cầu (hoặc tái cấu hình), trong đó một bên (chẳng hạn, thiết bị mạng) xác định danh sách tùy chọn khả dụng để cho phép bên ngược lại (chẳng hạn, thiết bị truyền thông) chọn tùy chọn so khớp tốt nhất (tức là, đúng bộ phận bảo mật), nhờ đó giảm các sai khớp bộ phận bảo mật, và cải thiện toàn bộ bảo mật mạng và hiệu suất trong quản lý mạng.

Theo dạng triển khai thứ năm theo khía cạnh thứ hai, phương pháp còn bao gồm bước kiểm chứng, bởi thiết bị truyền thông, quyết định liên quan đến gia nhập bộ phận bảo mật thứ hai dựa trên đánh giá của tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai. Phương pháp còn bao gồm bước điều khiển, bởi thiết bị truyền thông, kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông theo tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai, nếu kiểm chứng thành công.

Phương pháp tạo cơ hội cho thiết bị truyền thông đánh giá tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai, để quyết định liệu bộ phận bảo mật thứ hai có thỏa mãn thay đổi trong tiểu sử bảo mật thứ nhất (chẳng hạn, thay đổi do sự cố tường lửa nội bộ ở thiết bị truyền thông). Điều này có thể tham gia chủ động của thiết bị truyền thông cùng với thiết bị mạng trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật (chẳng hạn, bộ phận bảo mật thứ hai được xác định trong trường hợp này).

Ở dạng triển khai thứ sáu theo khía cạnh thứ hai, thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất dựa trên hoạt động gia nhập lần đầu tiên giữa thiết bị truyền thông và thiết bị mạng. Hoạt động gia nhập lần đầu tiên bao gồm bước cung cấp, bởi thiết bị truyền thông, tiểu sử bảo mật thứ nhất cho

thiết bị mạng theo bộ phận thương lượng khi thiết bị truyền thông ở trạng thái không được phân định cho bộ phận bảo mật cụ thể. Tiểu sử bảo mật thứ nhất chỉ báo các khả năng của thiết bị và các yêu cầu bảo mật của thiết bị truyền thông ở trạng thái không được phân định. Hoạt động gia nhập lần đầu tiên còn bao gồm thu được, bởi thiết bị truyền thông, lệnh từ thiết bị mạng để gia nhập bộ phận bảo mật thứ nhất. Hoạt động gia nhập lần đầu tiên còn bao gồm gia nhập, bởi thiết bị truyền thông, bộ phận bảo mật thứ nhất dựa trên lệnh thu được.

Trong trường hợp trong đó thiết bị truyền thông chưa được phân định cho bộ phận bảo mật bất kỳ (tức là, trạng thái không được phân định), hoạt động gia nhập lần đầu tiên khiến thiết bị mạng có thể xác định, dựa trên tiểu sử bảo mật thứ nhất, bộ phận bảo mật so khớp tốt nhất (tức là, bộ phận bảo mật thứ nhất) từ trong số các bộ phận bảo mật để phân định cho thiết bị truyền thông, nhờ đó bảo mật đầy đủ. Chẳng hạn, các đặc tính bảo mật cụ thể (hoặc thuộc tính bảo mật) của thiết bị truyền thông mà bên cạnh đó có thể vẫn chưa được dò thấy (tức là, không bị lộ) qua kênh truyền thông thông thường (chẳng hạn, sử dụng chức năng tự phát hiện) giữa thiết bị truyền thông và thiết bị mạng, được dò thấy dễ dàng và chính xác nhờ sử dụng tiểu sử bảo mật thứ nhất.

Theo khía cạnh thứ ba, sáng chế đề cập đến thiết bị mạng thực hiện thương lượng bảo mật cho cấu hình mạng. Thiết bị mạng bao gồm mạch điều khiển được tạo cấu hình để thu được thông tin cập nhật bảo mật từ thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất. Bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Mạch điều khiển còn được tạo cấu hình để xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông dựa trên thông tin cập nhật bảo mật. Mạch điều khiển còn được tạo cấu hình để cấp lệnh cho thiết bị truyền thông để gia nhập bộ phận bảo mật thứ hai được xác định.

Theo các dạng triển khai nữa của thiết bị mạng của khía cạnh thứ ba, mạch điều khiển được tạo cấu hình để thực hiện các đặc điểm của các dạng triển khai của phương pháp theo khía cạnh thứ nhất. Do vậy, các dạng triển khai của thiết

bị mạng bao gồm (các) đặc điểm của dạng triển khai tương ứng của phương pháp theo khía cạnh thứ nhất.

Thiết bị mạng theo khía cạnh thứ ba đạt đến tất cả các ưu điểm và các hiệu quả của phương pháp theo khía cạnh thứ nhất.

Theo khía cạnh thứ tư, sáng chế đề cập đến thiết bị truyền thông thực hiện thương lượng bảo mật cho cấu hình mạng. Thiết bị truyền thông bao gồm mạch điều khiển được tạo cấu hình để cấp thông tin cập nhật bảo mật cho thiết bị mạng từ thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất. Bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Mạch điều khiển còn được tạo cấu hình để thu được lệnh từ thiết bị mạng để gia nhập bộ phận bảo mật thứ hai. Mạch điều khiển còn được tạo cấu hình để gia nhập bộ phận bảo mật thứ hai thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông, dựa trên lệnh thu được.

Theo các dạng triển khai khác của thiết bị truyền thông theo khía cạnh thứ tư, mạch điều khiển được tạo cấu hình để thực hiện các dấu hiệu của các dạng triển khai của phương pháp theo khía cạnh thứ hai. Do vậy, các dạng triển khai của thiết bị truyền thông bao gồm (các) dấu hiệu của dạng triển khai tương ứng của phương pháp theo khía cạnh thứ hai.

Thiết bị truyền thông theo khía cạnh thứ tư đạt đến tất cả các ưu điểm và các hiệu quả của phương pháp theo khía cạnh thứ hai.

Theo khía cạnh thứ năm, sáng chế đề cập đến sản phẩm chương trình máy tính bao gồm vật ghi máy tính đọc được bất biến có các lệnh máy tính đọc được được lưu trữ trên đó, các lệnh máy tính đọc được sẽ được thực thi bằng thiết bị máy tính bao gồm phần cứng xử lý để thực thi phương pháp nêu trên theo khía cạnh thứ nhất hoặc khía cạnh thứ hai.

Sản phẩm chương trình máy tính theo khía cạnh thứ năm đạt đến tất cả các ưu điểm và các hiệu quả của phương pháp theo khía cạnh thứ nhất hoặc khía cạnh thứ hai.

Cần lưu ý rằng tất cả các thiết bị, phần tử, hệ mạch, khối và phương tiện được mô tả trong bản mô tả có thể được thực hiện bằng phần mềm hoặc các linh kiện phần cứng hoặc bất kỳ tổ hợp nào của nó. Tất cả các bước được thực hiện bởi các thực thể khác nhau được nêu trong bản mô tả cũng như các chức năng được mô tả được thực hiện bởi các thực thể khác nhau sẽ có nghĩa là thực thể tương ứng được thích ứng với hoặc được tạo cấu hình để thực hiện các bước và các chức năng tương ứng. Thậm chí nếu, trong phần mô tả sau của các phương án thực hiện cụ thể, chức năng hoặc bước cụ thể được thực hiện bởi các thực thể bên ngoài không được phản ánh trong phần mô tả của phần tử được mô tả chi tiết của thực thể đó mà thực hiện bước hoặc chức năng cụ thể, người có hiểu biết trung bình trong lĩnh vực cần hiểu rằng các phương pháp và các chức năng có thể được thực hiện trong phần mềm hoặc các linh kiện phần cứng, hoặc loại kết hợp bất kỳ của chúng. Cần hiểu rằng các dấu hiệu của sáng chế dễ được kết hợp trong các tổ hợp khác nhau mà không xa rời phạm vi của sáng chế như được định nghĩa bởi các điểm yêu cầu bảo hộ đi kèm.

Các khía cạnh, các ưu điểm, các dấu hiệu và các đối tượng bổ sung của sáng chế sẽ trở nên rõ ràng trong hình vẽ và phần mô tả chi tiết của các cách thực hiện minh họa được hiểu dựa vào các điểm yêu cầu bảo hộ đi kèm dưới đây.

Mô tả vắn tắt các hình vẽ

Phần bản chất nêu trên, cũng như phần mô tả chi tiết dưới đây của các phương án thực hiện minh họa, được hiểu rõ hơn dựa vào các hình vẽ đi kèm. Để minh họa sáng chế, các cấu thành lấy làm ví dụ của sáng chế được thể hiện trên hình vẽ. Tuy nhiên, sáng chế không bị giới hạn ở các phương pháp cụ thể và các phương tiện được bộc lộ ở đây. Ngoài ra, người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rằng các hình vẽ không theo tỷ lệ. Bất cứ chỗ nào có thể, các phần tử tương tự đã được chỉ báo bằng các số giống hệt.

Các phương án thực hiện sáng chế sẽ được mô tả, chỉ thông qua ví dụ, dựa vào các sơ đồ dưới đây trong đó:

Fig.1 là lưu đồ của phương pháp thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị mạng, theo phương án thực hiện sáng chế;

Fig.2 là lưu đồ của phương pháp thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị truyền thông, theo phương án thực hiện sáng chế;

Fig.3A là sơ đồ môi trường mạng của hệ thống có thiết bị mạng và thiết bị truyền thông, theo phương án thực hiện sáng chế;

Fig.3B là sơ đồ khối minh họa các thành phần lấy làm ví dụ khác nhau của thiết bị mạng, theo phương án thực hiện sáng chế;

Fig.3C là sơ đồ khối minh họa các thành phần lấy làm ví dụ khác nhau của thiết bị truyền thông, theo phương án thực hiện sáng chế;

Fig.4 là sơ đồ minh họa truyền thông lấy làm ví dụ giữa thiết bị mạng và thiết bị truyền thông để thực thi thương lượng bảo mật để cấu hình mạng, theo phương án thực hiện sáng chế;

Fig.5 là hình vẽ minh họa kịch bản lấy làm ví dụ mô tả nguyên lý hoạt động thương lượng bảo mật để cấu hình mạng, theo phương án thực hiện sáng chế; và

Fig.6 là hình vẽ minh họa kịch bản lấy làm ví dụ mô tả thực thi thương lượng bảo mật để cấu hình mạng cho các thiết bị truyền thông khác nhau, theo phương án thực hiện sáng chế.

Trong các hình vẽ đi kèm, số gạch chân được sử dụng để biểu diễn hạng mục trên đó số gạch chân được định vị hoặc hạng mục mà số được gạch chân liền kề. Số không gạch chân liên quan đến hạng mục được nhận diện bằng đường thẳng nối số không gạch chân với hạng mục này. Khi số không được gạch chân và đi kèm mũi tên liên kết, thì số không gạch chân được sử dụng để nhận diện hạng mục chung mà mũi tên trỏ đến.

Mô tả chi tiết sáng chế

Phần mô tả chi tiết sau minh họa các phương án thực hiện sáng chế và các cách trong đó chúng có thể được thực hiện. Mặc dù một số chế độ thực hiện sáng chế đã được bộc lộ, song người có hiểu biết trung bình trong lĩnh vực sẽ nhận ra rằng các phương án thực hiện khác để thực hiện sáng chế cũng khả thi.

Fig.1 là lưu đồ của phương pháp 100 thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị mạng, theo phương án thực hiện sáng chế. Phương pháp 100 được thực thi bằng thiết bị mạng được mô tả, chẳng hạn, trên Fig.3A. Phương pháp 100 bao gồm các bước 102, 104, và 106.

Ở bước 102, thông tin cập nhật bảo mật thu được bởi thiết bị mạng từ thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất. Bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Trong ví dụ, bộ phận bảo mật thứ nhất cũng có thể được gọi là bộ phận mạng (tức là, một trong nhiều bộ phận mạng ban đầu được phân định cho thiết bị truyền thông). Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất (chẳng hạn, tiểu sử bảo mật thiết bị) của thiết bị truyền thông. Chẳng hạn, tiểu sử bảo mật thứ nhất của thiết bị truyền thông có thể được thay đổi như là kết quả của sự cố ứng dụng tường lửa nội bộ ở thiết bị truyền thông. Trong ví dụ, thông tin cập nhật bảo mật thu được bởi thiết bị mạng dựa trên yêu cầu từ thiết bị truyền thông (tức là, yêu cầu xuất phát từ thiết bị truyền thông) để cấp phát lại bộ phận từ bộ phận bảo mật thứ nhất đang được phân định đến bộ phận bảo mật mới. Các ví dụ của thiết bị truyền thông, thiết bị mạng, và các tiểu sử bảo mật và các bộ phận khác nhau còn được mô tả chi tiết, chẳng hạn, trên Fig.3A và Fig.5.

Theo phương án thực hiện, tiểu sử bảo mật thứ nhất bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông, hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông. Tiểu sử bảo mật thứ nhất được cập nhật bởi thiết bị truyền thông thành tiểu sử bảo mật thứ hai dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hoặc thay đổi trong môi trường mạng của thiết bị truyền thông. Các ví dụ của các thuộc tính thiết bị bao gồm, nhưng không bị giới hạn ở loại thiết bị, tên nhà sản xuất, danh sách truy nhập hiện tại của bộ định vị tài nguyên đồng nhất (uniform resource locator, URL), danh sách của các giao thức (chẳng hạn, IPV4 hoặc IPV6) được hỗ trợ ở thiết bị truyền thông, danh sách của các cổng mở, danh sách của các cổng đóng, danh sách của các giao diện điều khiển được phép, loại nội dung đến và từ thiết

bị truyền thông, thuộc tính bảo mật của thiết bị truyền thông, và tương tự. Trong ví dụ, trạng thái hoạt động của thiết bị xác định trạng thái ứng dụng hoặc trạng thái phần cứng của thiết bị truyền thông khi đang vận hành. Môi trường mạng của thiết bị truyền thông bao gồm thông tin liên quan đến (các) đường kết nối mạng hiện tại được sử dụng bởi thiết bị truyền thông. Trong ví dụ, liệu lưu lượng dữ liệu đến và từ thiết bị truyền thông được định tuyến qua thiết bị mạng hoặc không được xác định tiềm năng trong (hoặc được suy ra từ) tiểu sử bảo mật thứ nhất. Ngược lại với các hệ thống và các phương pháp đã biết, tiểu sử bảo mật thứ nhất của thiết bị truyền thông động (và không tĩnh), có thể bao gồm (các) thay đổi như là kết quả thay đổi trong trạng thái hoạt động của thiết bị hoặc môi trường mạng của thiết bị truyền thông.

Theo phương án thực hiện, thông tin cập nhật bảo mật tương ứng với ít nhất một trong: tiểu sử bảo mật thứ hai hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất. Theo phương án thực hiện, toàn bộ tiểu sử bảo mật thứ hai được cấp cho thiết bị mạng. Nói cách khác, tiểu sử bảo mật thứ hai bị lộ (chẳng hạn, được quảng cáo hoặc công bố) sao cho thiết bị mạng có thể thu được tiểu sử bảo mật thứ hai. Theo phương án thực hiện khác, một cách tùy chọn, chỉ các thay đổi hoặc các cập nhật mới nhất (tức là, một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất) được cấp dưới dạng thông tin cập nhật bảo mật cho thiết bị mạng để tiết kiệm băng thông mạng, và cải thiện hiệu năng mạng. Tiểu sử bảo mật thứ hai bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông, yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ trong bộ phận bảo mật thứ nhất được phân định cho thiết bị truyền thông, hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông. Trong các hệ thống và các phương pháp đã biết, các thay đổi liên quan đến các yêu cầu bảo mật ở thiết bị truyền thông không được phản ánh ngay lập tức bởi các mẫu hình truyền thông mạng, và do vậy thiết bị mạng đã biết không nhận biết được về các thay đổi này. Ngược lại với các hệ thống và các phương pháp đã biết, các

thay đổi này có thể nhận thức được từ thông tin cập nhật bảo mật thu được, nhờ đó giảm rủi ro của các lỗ hổng bảo mật trong thiết bị truyền thông và cải thiện toàn bộ bảo mật mạng và hiệu suất trong quản lý mạng.

Theo phương án thực hiện, thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất dựa trên hoạt động gia nhập lần đầu tiên giữa thiết bị mạng và thiết bị truyền thông. Hoạt động gia nhập lần đầu tiên bao gồm thu được, bởi thiết bị mạng, tiểu sử bảo mật thứ nhất từ thiết bị truyền thông theo bộ phận thương lượng khi thiết bị truyền thông ở trạng thái không được phân định cho bộ phận bảo mật cụ thể. Trong ví dụ, bộ phận thương lượng có thể đề cập đến bộ phận mạng hỗ trợ thương lượng bảo mật và tạm thời được sử dụng bởi thiết bị mạng và thiết bị truyền thông để truyền thông trước khi thực sự phân định (hoặc cấp phát) bộ phận bảo mật cụ thể trong các bộ phận bảo mật. Tiểu sử bảo mật thứ nhất chỉ báo các khả năng của thiết bị và các yêu cầu bảo mật của thiết bị truyền thông ở trạng thái không được phân định. Hoạt động gia nhập lần đầu tiên còn bao gồm xác định, bởi thiết bị mạng, bộ phận bảo mật thứ nhất từ các bộ phận bảo mật để phân định cho thiết bị truyền thông dựa trên tiểu sử bảo mật thứ nhất thu được. Hoạt động gia nhập lần đầu tiên còn bao gồm bước tạo, bởi thiết bị mạng, lệnh cho thiết bị truyền thông để gia nhập bộ phận bảo mật thứ nhất. Lệnh thông báo thiết bị truyền thông về bộ phận bảo mật thứ nhất được xác định liên quan đến các khả năng thiết bị và các yêu cầu bảo mật của thiết bị truyền thông.

Ở bước 104, bộ phận bảo mật thứ hai được xác định bởi thiết bị mạng đối với thiết bị truyền thông dựa trên thông tin cập nhật bảo mật. Bộ phận bảo mật thứ hai được xác định là bộ phận thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Theo phương án thực hiện, việc xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông bao gồm bước so sánh các thuộc tính bảo mật được liên kết với ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất với các thuộc tính bảo mật tương ứng được liên kết với mỗi tiểu sử trong các tiểu sử bảo mật bộ phận được liên kết với các bộ phận bảo mật. Việc so sánh được thực thi để tìm ra bộ phận so khớp tốt nhất (tức là, bộ phận bảo mật thứ hai trong trường hợp này) đối với

thiết bị truyền thông từ trong số các bộ phận bảo mật đối với thiết bị truyền thông.

Theo phương án thực hiện, việc xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông bao gồm việc sử dụng bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ hai. Trong ví dụ, bộ chỉ báo loại tin nhắn có thể chỉ báo theo yêu cầu để cấp phát lại bộ phận.

Ở bước 106, lệnh được cấp bởi thiết bị mạng cho thiết bị truyền thông để gia nhập bộ phận bảo mật thứ hai được xác định. Nói cách khác, thiết bị mạng ra lệnh cho thiết bị truyền thông gia nhập (tức là, kích hoạt gia nhập) vào bộ phận bảo mật phù hợp.

Theo phương án thực hiện, phương pháp 100 còn bao gồm bước cấp, bởi thiết bị mạng, cho thiết bị truyền thông, tiểu sử bảo mật bộ phận thứ hai được liên kết với bộ phận bảo mật thứ hai được xác định. Tiểu sử bảo mật bộ phận thứ hai được sử dụng bởi thiết bị truyền thông để kiểm chứng quyết định để gia nhập bộ phận bảo mật thứ hai. Thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai nếu kiểm chứng thành công (tức là thiết bị truyền thông và thiết bị mạng cùng thỏa hiệp rằng bộ phận bảo mật thứ hai là so khớp tốt nhất theo thông tin cập nhật bảo mật). Tiểu sử bảo mật bộ phận thứ hai còn được sử dụng bởi thiết bị truyền thông để điều khiển, dựa trên kiểm chứng, kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông theo tiểu sử bảo mật bộ phận thứ hai. Nói cách khác, trong trường hợp trong đó kiểm chứng thành công, các chức năng hoặc các dịch vụ cụ thể ở thiết bị truyền thông (đã trở nên không tương thích như là kết quả thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông) được kích hoạt hoặc vô hiệu hóa (chẳng hạn, các chức năng không bảo mật có thể bị vô hiệu hóa) theo tiểu sử bảo mật bộ phận thứ hai.

Theo phương án thực hiện, phương pháp 100 còn bao gồm áp dụng chính sách mạng cụ thể được liên kết với bộ phận bảo mật thứ hai đối với thiết bị truyền thông sau khi thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai và rời khỏi bộ phận bảo mật thứ nhất. Trong ví dụ, thiết bị mạng có thể bao gồm chức năng của bộ quản lý chính sách mà quản lý các chính sách mạng khác

nhau được liên kết với các bộ phận bảo mật khác nhau. Bộ phận bảo mật cụ thể có chính sách mạng cụ thể được liên kết với chúng. Sau khi thực thi thương lượng bảo mật, và thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai được xác định, chính sách mạng cụ thể liên quan đến bộ phận bảo mật thứ hai được áp dụng để chủ động lấp đầy khe hở bảo mật tiềm năng có thể phát sinh do thay đổi mới nhất trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông.

Các bước 102, 104, và 106 chỉ là minh họa và các tùy chọn khác cũng có thể được cấp trong đó một hoặc nhiều bước được bổ sung, một hoặc nhiều bước được loại bỏ, hoặc một hoặc nhiều bước được bố trí trong chuỗi khác mà không xa rời phạm vi của các điểm yêu cầu bảo hộ ở đây.

Fig.2 là lưu đồ của phương pháp 200 thực thi thương lượng bảo mật để tạo cấu hình mạng ở thiết bị truyền thông, theo phương án thực hiện sáng chế. Phương pháp 200 được thực thi bằng thiết bị truyền thông được mô tả, chẳng hạn, trên Fig.3A.

Ở bước 202, thông tin cập nhật bảo mật được cấp cho thiết bị mạng bởi thiết bị truyền thông. Thiết bị truyền thông được phân định cho bộ phận bảo mật thứ nhất được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Do thông tin cập nhật bảo mật được chủ động chia sẻ bởi thiết bị truyền thông với thiết bị mạng, việc chủ động tham gia của thiết bị truyền thông được đảm bảo trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật của thiết bị truyền thông. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông. Theo phương án thực hiện, tiểu sử bảo mật thứ nhất bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông, hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông.

Theo phương án thực hiện, thông tin cập nhật bảo mật được cấp bởi thiết bị truyền thông cho thiết bị mạng dựa trên thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hoặc thay đổi trong môi trường mạng của thiết bị truyền thông. Theo phương án thực hiện, thông tin cập nhật bảo mật tương ứng với ít nhất một trong: tiểu sử bảo mật thứ hai hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất. Tiểu sử bảo mật

thứ hai bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông, yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ bởi bộ phận bảo mật thứ nhất, hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông. Bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ hai được sử dụng bởi thiết bị mạng để xác định bộ phận bảo mật thứ hai.

Ở bước 204, lệnh thu được bởi thiết bị truyền thông từ thiết bị mạng để gia nhập bộ phận bảo mật thứ hai. Thông tin cập nhật bảo mật được cấp bởi thiết bị truyền thông khiến thiết bị mạng có thể nhận thức bất kỳ thay đổi trong các chức năng và các hoạt động liên quan đến mạng thậm chí nếu bất kỳ truyền thông liên quan đến mạng nào bỏ qua kênh truyền thông thông thường với thiết bị mạng. Do vậy, thiết bị mạng có thể xác định bộ phận bảo mật thích hợp (tức là, bộ phận bảo mật thứ hai trong trường hợp này), và gửi lệnh đến thiết bị truyền thông để gia nhập bộ phận bảo mật thứ hai được xác định.

Ở bước 206, bộ phận bảo mật thứ hai thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông, được gia nhập bởi thiết bị truyền thông dựa trên lệnh thu được. Việc gia nhập bộ phận bảo mật thứ hai bởi thiết bị truyền thông có thể đóng nhanh chóng và đầy đủ các khe hở bảo mật có thể tiềm tàng phát sinh do cập nhật hoặc thay đổi (chẳng hạn, các thay đổi trong các thuộc tính bảo mật, dịch vụ, hoặc thuộc tính cụ thể) trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông.

Theo phương án thực hiện, việc gia nhập bộ phận bảo mật thứ hai bao gồm thu được, bởi thiết bị truyền thông, từ thiết bị mạng, một hoặc nhiều trong số: danh sách dịch vụ bảo mật được hỗ trợ bởi thiết bị mạng cho bộ phận bảo mật thứ hai, tiểu sử bảo mật bộ phận thứ hai được liên kết với bộ phận bảo mật thứ hai, hoặc các tiểu sử bảo mật bộ phận cho các bộ phận bảo mật khả dụng với thiết bị mạng. Nói cách khác, thông tin này (chẳng hạn danh sách các dịch vụ bảo mật, tiểu sử bảo mật bộ phận thứ hai, và các tiểu sử bảo mật bộ phận khả dụng khác) thu được từ thiết bị mạng có thể thương lượng bảo mật và kiểm

chứng bảo mật lẫn nhau giữa thiết bị truyền thông và thiết bị mạng. Cả thiết bị mạng và thiết bị truyền thông có thể thực thi thương lượng bảo mật, trong đó một bên (chẳng hạn, thiết bị mạng) xác định danh sách của các tùy chọn khả dụng để cho phép bên kia (chẳng hạn, thiết bị truyền thông) chọn tùy chọn khớp nhất (tức là, đúng bộ phận bảo mật), nhờ đó giảm sai khớp bộ phận bảo mâtes, và cải thiện toàn bộ bảo mật mạng và hiệu suất trong quản lý mạng.

Theo phương án thực hiện, việc gia nhập bộ phận bảo mật thứ hai còn bao gồm kiểm chứng, bởi thiết bị truyền thông, quyết định liên quan đến gia nhập of bộ phận bảo mật thứ hai dựa trên đánh giá của tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai. Thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai nếu kiểm chứng thành công (tức là, thiết bị truyền thông và thiết bị mạng thỏa thuận với nhau rằng bộ phận bảo mật thứ hai là so khớp tốt nhất theo thông tin cập nhật bảo mật. Việc kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông được điều khiển theo tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai, nếu kiểm chứng thành công. Chẳng hạn, thiết bị truyền thông có thể vô hiệu hóa các cập nhật firmware qua mạng Wi-Fi nếu thiết bị mạng (chẳng hạn, bộ định tuyến) không hỗ trợ bộ phận bảo mật dành riêng cho chức năng này do việc cập nhật firmware qua mạng phẳng (chẳng hạn, mạng trong đó tất cả các thiết bị truyền thông được nối qua cùng thiết bị mạng) được xem xét là không bảo mật đối với thiết bị truyền thông.

Theo phương án thực hiện, phương pháp 200 còn bao gồm bước cập nhật, bởi thiết bị truyền thông, tiểu sử bảo mật thứ nhất thành tiểu sử bảo mật thứ hai dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông hoặc thay đổi trong môi trường mạng của thiết bị truyền thông.

Các bước 202, 204, và 206 chỉ là minh họa và các tùy chọn khác cũng có thể được đề xuất trong đó bổ sung một hoặc nhiều bước, một hoặc nhiều bước được loại bỏ, hoặc một hoặc nhiều bước được bố trí trong trình tự khác mà không xa rời phạm vi của các điểm yêu cầu bảo hộ ở đây.

Fig.3A là sơ đồ môi trường mạng của hệ thống 300 có thiết bị mạng và thiết bị truyền thông, theo phương án thực hiện sáng chế. Dựa vào Fig.3A, môi

trường mạng của hệ thống 300 được thể heiện bao gồm thiết bị mạng 302 và thiết bị truyền thông 304. Ngoài ra còn thể hiện mạng truyền thông thứ nhất 306, mạng truyền thông thứ hai 308, và đường kết nối mạng thay thế 310.

Thiết bị mạng 302 đề cập đến phần cứng kết nối mạng hoạt động như là cổng nối hoặc phương tiện trung gian giữa hai mạng, chẳng hạn mạng truyền thông thứ nhất 306 và mạng truyền thông thứ hai 308. Chẳng hạn, thiết bị truyền thông 304 có thể được ghép nối truyền thông với thiết bị mạng 302 qua mạng truyền thông thứ nhất 306 (chẳng hạn, mạng cục bộ không dây (wireless local area network, WLAN)). Thiết bị truyền thông 304 có thể truy nhập mạng truyền thông thứ hai 308 (chẳng hạn, mạng Internet) qua thiết bị mạng 302. Thiết bị mạng 302 bao gồm các tiểu sử bảo mật bộ phận được liên kết với các bộ phận bảo mật. Các bộ phận bảo mật là các đoạn khác nhau của mạng (chẳng hạn, mạng truyền thông thứ nhất 306) được tách khỏi các bộ phận khác bởi thiết bị mạng 302. Các bộ phận bảo mật cũng có thể được gọi là các bộ phận mạng được tạo sau khi phân đoạn mạng. Phân đoạn mạng là tách mạng truyền thông thành các mạng thành phần, trong đó mỗi mạng thành phần được gọi là bộ phận bảo mật (bộ phận mạng). Các ví dụ về thiết bị mạng 302 bao gồm, nhưng không bị giới hạn ở thiết bị cổng nối thường trú, bộ định tuyến, bộ định tuyến cầu nối (tức là, brouter), bộ điều khiển mạng, thiết bị truy nhập không dây cố định (fixed wireless access, FWA), máy chủ, thiết bị tường lửa, haowjc thiết bị bảo mật mạng.

Theo phương án thực hiện, thiết bị mạng 302 có thể bao gồm các giao diện lập trình ứng dụng riêng cho thương lượng bảo mật (application programming interface, API) hỗ trợ xác thực và mật mã hóa dữ liệu để chống lại các địch thủ tiềm tàng trên mạng. Thiết bị truyền thông 304 cũng có thể bao gồm các API tương thích này để hỗ trợ thương lượng bảo mật với thiết bị mạng 302. Chẳng hạn, các yêu cầu và dữ liệu đến và từ thiết bị truyền thông 304 và thiết bị mạng 302 có thể được mật mã hóa và một cách tùy chọn được ký số để đảm bảo tính bí mật, toàn vẹn, và đáng tin cậy của thông tin được cấp.

Thiết bị truyền thông 304 có thể bao gồm lôgic thích hợp, hệ mạch, các giao diện và/hoặc mã được tạo cấu hình để truyền thông với thiết bị mạng 302

qua mạng truyền thông thứ nhất 306. Các ví dụ của thiết bị truyền thông 304 bao gồm, nhưng không bị giới hạn ở điện thoại thông minh, thiết bị Internet vạn vật (Internet-of-Things, IoT), máy tính xách tay, máy tính bảng, máy tính cá nhân, thiết bị truyền thông loại máy (machine type communication, MTC), thiết bị kết nối kép NR truy nhập vô tuyến từ mặt đất của hệ thống viễn thông di động toàn cầu tiến hóa (((evolved universal mobile telecommunications system, UMTS) terrestrial radio access, E-UTRAN) NR-dual connectivity, EN-DC), máy chủ, bộ điều khiển IoT, máy bay không người lái (drone), thiết bị điện toán cầm tay, phần cứng được tùy chỉnh để truyền thông không dây, hoặc các thiết bị điện tử mang đi được hoặc không mang đi được khác bất kỳ.

Mạng truyền thông thứ nhất 306 có thể bao gồm phương tiện qua đó một hoặc nhiều thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304 có thể truyền thông với thiết bị mạng 302. Các ví dụ về mạng truyền thông thứ nhất 306 có thể bao gồm, nhưng không bị giới hạn ở, mạng tầm ngắn (chẳng hạn, mạng tại gia), mạng tần số vô tuyến hai chiều (chẳng hạn, mạng dựa trên Bluetooth), mạng diện cá nhân không dây (Wireless Personal Area Network, WPAN), và/hoặc WLAN, chẳng hạn, mạng không dây (Wireless Fidelity, Wi-Fi). Các thiết bị truyền thông khác nhau, chẳng hạn thiết bị truyền thông 304, có thể được tạo cấu hình để kết nối với thiết bị mạng 302, trong mạng truyền thông thứ nhất 306, theo các giao thức truyền thông hữu tuyến hoặc không dây khác nhau. Các ví dụ về các giao thức truyền thông hữu tuyến hoặc không dây này hoặc các chuẩn kỹ thuật có thể bao gồm, nhưng không bị giới hạn ở, ủy ban kỹ thuật của tổ chức chuẩn hóa quốc tế (International Organization for Standardization's (ISO) Technical Committee, TC) 16058, giao thức Bluetooth, giao thức hồng ngoại, giao thức không dây (Wireless Fidelity, Wi-Fi), giao thức ZigBee, IEEE 802.11, 802.16, giao thức truyền thông tế bào, giao thức truyền thông trường gần (Near Field Communication, NFC), giao thức buýt nối tiếp đa năng (Universal Serial Bus, USB), và/hoặc giao thức USB không dây.

Trong ví dụ, mạng truyền thông thứ hai 308 có thể khác với mạng truyền thông thứ nhất 306. Mạng truyền thông thứ hai 308 có thể được truy nhập bởi một hoặc nhiều thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304, qua

thiết bị mạng 302, hoạt động như là bộ phận trung gian hoặc cổng nối giữa mạng truyền thông thứ nhất 306 và mạng truyền thông thứ hai 308. Trong một số trường hợp, mạng truyền thông thứ hai 308 có thể được truy nhập trực tiếp bởi một hoặc nhiều thiết bị truyền thông bỏ qua thiết bị mạng 302 nhờ sử dụng đường kết nối mạng 310 tùy chọn. Các ví dụ về mạng truyền thông thứ hai 308 có thể bao gồm, nhưng không bị giới hạn ở, mạng Internet, mạng điện toán đám mây, mạng nội bộ (Local Area Network, LAN), đường điện thoại (POTS), mạng đô thị (Metropolitan Area Network, MAN), mạng bộ cảm biến không dây (wireless sensor network, WSN), và/hoặc mạng tế bào, chẳng hạn mạng 3G, 4G tiến hóa dài hạn (long-term evolution, LTE), hoặc mạng 5G. Các thiết bị khác nhau trong môi trường mạng có thể được tạo cấu hình để kết nối với mạng truyền thông thứ hai 308, theo các giao thức truyền thông không dây khaccs nhau. Các ví dụ về such các giao thức truyền thông không dây, các chuẩn truyền thông, và công nghệ có thể bao gồm, nhưng không bị giới hạn ở, IEEE 802.11, 802.11p, 802.15, 802.16, 1609, liên tác toàn cầu truy nhập vi sóng (Worldwide Interoperability for Microwave Access, Wi-MAX), giao thức điều khiển truyền và giao thức Internet (Transmission Control Protocol and Internet Protocol, TCP/IP), giao thức lượng dữ liệu người dùng (User Datagram Protocol, UDP), giao thức truyền siêu văn bản (Hypertext Transfer Protocol, HTTP), LTE, giao thức truyền tệp tin (File Transfer Protocol, FTP), môi trường GSM dữ liệu tăng cường (Enhanced Data GSM Environment, EDGE), giao thức thoại trên mạng Internet (voice over Internet Protocol, VoIP), giao thức cho thư điện tử, nhắn tin nhanh, và/hoặc dịch vụ tin nhắn ngắn (Short Message Service, SMS), và/hoặc các giao thức truyền thông tế bào.

Đường kết nối mạng tùy chọn 310 đề cập đến kênh truyền thông (hoặc đường kết nối) để kết nối với mạng (chẳng hạn, mạng truyền thông thứ hai 308) bỏ qua thiết bị mạng 302. Chẳng hạn, thiết bị truyền thông 304 có thể được ghép nối truyền thông với thiết bị mạng 302 qua mạng Wi-Fi (chẳng hạn, mạng truyền thông thứ nhất 306) và có thể truy nhập Internet (chẳng hạn, mạng truyền thông thứ hai 308) qua thiết bị mạng 302. Trong các kịch bản cụ thể,

thiết bị truyền thông 304 có thể truy nhập trực tiếp mạng Internet qua mạng tế bào bỏ qua kênh truyền thông thông thường (chẳng hạn, mạng Wi-Fi). Do vậy, mạng tế bào tương ứng với đường kết nối mạng tùy chọn 310 trong trường hợp này.

Theo phương án thực hiện, thiết bị truyền thông 304 bao gồm tiểu sử bảo mật thứ nhất (tức là, tiểu sử bảo mật thiết bị). Tiểu sử bảo mật thứ nhất bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông 304, hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông 304. Tiểu sử bảo mật thứ nhất có cấu trúc dữ liệu bao gồm các trường. Mỗi trường trong các trường bao gồm thuộc tính bảo mật. Trong ví dụ, các thuộc tính thiết bị định nghĩa các thuộc tính bảo mật, chẳng hạn loại thiết bị, tên nhà sản xuất, danh sách truy nhập hiện tại của các URL, danh sách của các giao thức (chẳng hạn, IPV4 hoặc IPV6) được hỗ trợ ở thiết bị truyền thông 304, danh sách của các cổng mở, danh sách của các cổng đóng, danh sách của các giao diện điều khiển được phép và loại nội dung đến và từ thiết bị truyền thông 304, và thuộc tính bảo mật của thiết bị truyền thông 304. Cụm từ 'thuộc tính bảo mật' đề cập đến trạng thái bảo mật liên quan đến một hoặc nhiều phần mềm và phần cứng của thiết bị truyền thông 304. Thuộc tính bảo mật có thể chỉ báo các điều khiển hiện tại và các biện pháp được thực hiện ở thiết bị truyền thông 304 để bảo vệ thiết bị truyền thông 304 và các thiết bị khác, truyền thông với thiết bị truyền thông 304. Chẳng hạn, thuộc tính bảo mật của thiết bị truyền thông 304 có thể xác định các thiết lập cấu hình hiện tại và các cấp quyền liên quan đến các ứng dụng được cài đặt trước và hệ điều hành ở thiết bị truyền thông 304, danh sách của các dịch vụ chạy ở thiết bị truyền thông 304, danh sách của các dịch vụ bị vô hiệu hóa ở thiết bị truyền thông 304, các cấu hình khôi phục dữ liệu, các thành phần phần cứng được kích hoạt hoặc vô hiệu hóa, và các thành phần phụ trợ được hỗ trợ ở thiết bị truyền thông 304.

Trong ví dụ, trạng thái hoạt động của thiết bị xác định trạng thái ứng dụng hoặc trạng thái phần cứng của thiết bị truyền thông 304 khi đang vận hành. Chẳng hạn, trạng thái hoạt động của thiết bị có thể chỉ báo rằng ứng dụng

tường lửa nội bộ đang hoạt động và có các định nghĩa virut mới nhất. Môi trường mạng của thiết bị truyền thông 304 bao gồm thông tin liên quan đến (các) đường kết nối mạng hiện tại được sử dụng bởi thiết bị truyền thông 304. Chẳng hạn, nếu lưu lượng dữ liệu đến và từ thiết bị truyền thông 304 được định tuyến qua thiết bị mạng 302 qua mạng truyền thông thứ nhất 306 hoặc thiết bị truyền thông 304 đang truy nhập mạng truyền thông thứ hai 308 (chẳng hạn, Internet) trực tiếp qua đường nối tế bào (chẳng hạn, đường kết nối mạng tùy chọn 310). Trong ví dụ, môi trường mạng của thiết bị truyền thông 304 có thể cũng chỉ báo mẫu hình truyền thông của thiết bị truyền thông 304. Yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông 304 có thể bao gồm danh sách của các dịch vụ được yêu cầu thêm bởi thiết bị truyền thông 304. Yêu cầu truy nhập một hoặc nhiều dịch vụ có thể cũng bao gồm danh sách của các dịch vụ cần được vô hiệu hóa. Chẳng hạn, yêu cầu có thể xác định yêu cầu truy nhập tài nguyên mạng (chẳng hạn, truy nhập vào máy chủ dữ liệu, truy nhập vào thư mục mới trong máy chủ dữ liệu, truy nhập vào ứng dụng mới trong máy chủ dữ liệu hoặc máy chủ khác (chẳng hạn, máy chủ ứng dụng), loại quyền điều khiển truy nhập được xác định (tức là, đọc, ghi, chỉnh sửa, hoặc các quyền đặc biệt) đối với ổ mạng hoặc thư mục trong ổ mạng hoặc ổ nội bộ của thiết bị truyền thông 304, và tương tự.

Theo phương án thực hiện, thiết bị truyền thông 304 ở trạng thái không được phân định đến bộ phận bảo mật cụ thể. Trong trường hợp trong đó thiết bị truyền thông 304 ở trạng thái không được phân định (tức là, vẫn chưa được phân định cho bộ phận bảo mật bất kỳ bởi thiết bị mạng 302), hoạt động gia nhập lần đầu tiên được thực thi giữa thiết bị truyền thông 304 và thiết bị mạng 302. Trong hoạt động gia nhập lần đầu tiên, thiết bị truyền thông 304 được tạo cấu hình để cấp tiểu sử bảo mật thứ nhất cho thiết bị mạng 302 theo bộ phận thương lượng khi thiết bị truyền thông 304 ở trạng thái không được phân định. Như nêu trên, tiểu sử bảo mật thứ nhất chỉ báo các khả năng của thiết bị và các yêu cầu bảo mật của thiết bị truyền thông 304 ở trạng thái không được phân định. Trong ví dụ, bộ phận thương lượng có thể đề cập đến bộ phận mạng hỗ trợ thương lượng bảo mật và tạm thời được sử dụng bởi thiết bị mạng 302 và

thiết bị truyền thông 304 để truyền thông trước khi phân định thực (hoặc cấp phát) của bộ phận bảo mật trong các bộ phận bảo mật.

Theo phương án thực hiện, thiết bị mạng 302 được tạo cấu hình để thu được tiểu sử bảo mật thứ nhất từ thiết bị truyền thông 304 trên bộ phận thương lượng khi thiết bị truyền thông 304 ở trạng thái không được phân định. Thiết bị mạng 302 còn được tạo cấu hình để xác định bộ phận bảo mật thứ nhất từ các bộ phận bảo mật để phân định cho thiết bị truyền thông 304 dựa trên tiểu sử bảo mật thứ nhất thu được. Thiết bị mạng 302 còn được tạo cấu hình để cấp lệnh cho thiết bị truyền thông 304 để gia nhập bộ phận bảo mật thứ nhất. Lệnh thông báo thiết bị truyền thông 304 của bộ phận bảo mật thứ nhất được xác định liên quan đến các khả năng thiết bị và các yêu cầu bảo mật của thiết bị truyền thông 304.

Thiết bị truyền thông 304 còn được tạo cấu hình để thu được lệnh từ thiết bị mạng 302 để gia nhập bộ phận bảo mật thứ nhất. Thiết bị truyền thông 304 còn được tạo cấu hình để thu được tiểu sử bảo mật bộ phận thứ nhất được liên kết với bộ phận bảo mật thứ nhất. Tiểu sử bảo mật bộ phận thứ nhất có thể được sử dụng để đánh giá và kiểm chứng liệu bộ phận bảo mật thứ nhất có phù hợp theo tiểu sử bảo mật thứ nhất hay không chỉ báo các khả năng thiết bị và các yêu cầu bảo mật của thiết bị truyền thông 304. Do vậy, việc chủ động tham gia của thiết bị truyền thông 304 được đảm bảo trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật thứ nhất được xác định.

Thiết bị truyền thông 304 còn được tạo cấu hình để gia nhập bộ phận bảo mật thứ nhất dựa trên lệnh thu được. Do vậy, thiết bị truyền thông 304 được phân định cho bộ phận bảo mật thứ nhất dựa trên hoạt động gia nhập lần đầu tiên giữa thiết bị truyền thông 304 và thiết bị mạng 302. Trong các kịch bản cụ thể, trạng thái hoạt động của thiết bị của thiết bị truyền thông 304 hoặc môi trường mạng của thiết bị truyền thông 304, có thể thay đổi. Trong các kịch bản anỳ, thiết bị truyền thông 304 còn được tạo cấu hình để cập nhật tiểu sử bảo mật thứ nhất thành tiểu sử bảo mật thứ hai dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông 304 hoặc thay đổi trong môi trường mạng của thiết bị truyền thông 304. Theo phương án thực hiện, tiểu

sử bảo mật thứ hai bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông 304, yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ trong bộ phận bảo mật thứ nhất được phân định cho thiết bị truyền thông 304, hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông 304. Thông tin thay đổi động có thể liên quan đến thay đổi trong trạng thái ứng dụng hoặc trạng thái phần cứng (chẳng hạn, vô hiệu hóa đột ngột micrô hoặc kích hoạt camera gắn sẵn, nếu có) của thiết bị truyền thông.

Trong ví dụ, tiểu sử bảo mật thứ nhất của thiết bị truyền thông 304 có thể được cập nhật như là kết quả của sự cố ứng dụng tường lửa nội bộ. Trong ví dụ khác, thiết bị truyền thông 304 có thể là bộ điều khiển IoT. Ban đầu, bộ điều khiển IoT có thể truyền thông với các thiết bị IoT ngang hàng qua mạng truyền thông thứ nhất 306 (chẳng hạn, kênh Wi-Fi) qua thiết bị mạng 302. Có thể có thay đổi đột ngột của đường nối mạng, trong đó bộ điều khiển IoT có thể bắt đầu truyền thông với các thiết bị IoT ngang hàng và máy chủ đám mây trực tiếp qua mạng truyền thông thứ hai 308 (chẳng hạn, mạng tế bào), nhờ đó bỏ qua mạng truyền thông thứ nhất 306 (tức là, kênh Wi-Fi). Tiểu sử bảo mật thứ nhất có thể được cập nhật để phản ánh thay đổi này sao cho phiên truyền thông này bởi đường kết nối mạng tùy chọn 310 (tức là, mạng tế bào trong ví dụ này) là có thể nhận thức bởi thiết bị mạng 302. Trong ví dụ khác nữa, thiết bị truyền thông 304 có thể là thiết bị IoT. Đối với thiết bị IoT, ở thời gian cung cấp bảo mật, thiết bị IoT thường cần được ngắt kết nối khỏi mạng Wi-Fi (chẳng hạn, mạng truyền thông thứ nhất 306). Tiểu sử bảo mật thứ nhất có thể được cập nhật để phản ánh tạm thời cần ngắt kết nối. Trong các hệ thống và các phương pháp đã biết, các thay đổi này không được phản ánh ngay lập tức bởi các mẫu hình truyền thông mạng, và do vậy thiết bị mạng đã biết không nhận biết được về các thay đổi này. Ngoài ra, các thiết bị truyền thông đã biết có tiểu sử bảo mật tĩnh (tức là, tiểu sử thiết bị tĩnh). Ngược lại với các hệ thống và các phương

pháp đã biết, tiểu sử bảo mật thứ nhất của thiết bị truyền thông 304 là động, có thể chứa các thay đổi.

Đáp lại việc cập nhật tiểu sử bảo mật thứ nhất thành tiểu sử bảo mật thứ hai, thiết bị truyền thông 304 được tạo cấu hình để truyền yêu cầu đến thiết bị mạng 302. Yêu cầu có thể là yêu cầu để cấp phát lại bộ phận từ bộ phận bảo mật thứ nhất đang được phân định đến bộ phận bảo mật mới thích hợp theo ít nhất thay đổi trong tiểu sử bảo mật thứ nhất (chẳng hạn, thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông 304 hoặc thay đổi trong môi trường mạng của thiết bị truyền thông 304). Một cách tùy chọn, yêu cầu có thể được truyền ở dạng tin nhắn có bộ chỉ báo loại tin nhắn chỉ báo rằng yêu cầu là yêu cầu theo đòi hỏi để cấp phát lại bộ phận từ thiết bị truyền thông 304.

Thiết bị truyền thông 304 được tạo cấu hình để cấp thông tin cập nhật bảo mật cho thiết bị mạng 304. Thông tin cập nhật bảo mật được cấp bởi thiết bị truyền thông 304 khi thiết bị truyền thông 304 vẫn được phân định cho bộ phận bảo mật thứ nhất, được liên kết với tiểu sử bảo mật bộ phận thứ nhất. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông 304. Thiết bị mạng 302 được tạo cấu hình để thu được thông tin cập nhật bảo mật từ thiết bị truyền thông 304 được phân định cho bộ phận bảo mật thứ nhất.

Theo phương án thực hiện, thông tin cập nhật bảo mật tương ứng với ít nhất một trong tiểu sử bảo mật thứ hai hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất. Theo phương án thực hiện, toàn bộ tiểu sử bảo mật thứ hai được cấp cho thiết bị mạng 302 theo bộ phận thương lượng. Nói cách khác, tiểu sử bảo mật thứ hai bị lộ (chẳng hạn, được quảng cáo hoặc công bố như là tuyên bố) sao cho thiết bị mạng 302 có thể thu được tiểu sử bảo mật thứ hai. Theo phương án thực hiện khác, một cách tùy chọn, chỉ các thay đổi hoặc các cập nhật mới nhất (tức là, một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất) được cấp (hoặc bị lộ) dưới dạng thông tin cập nhật bảo mật cho thiết bị mạng 302 để tiết kiệm băng thông mạng, và cải thiện hiệu năng mạng. Theo phương án thực hiện này, thiết bị mạng 302 có thể lưu trữ tiểu sử bảo mật được nhận cuối cùng (chẳng hạn, tiểu

sử bảo mật thứ nhất) từ thiết bị truyền thông 304, và do vậy có thể dẫn xuất tiểu sử bảo mật thứ hai nhờ sử dụng (các) thay đổi mới nhất được nhận. Theo cách khác, do thiết bị mạng 302 đã có tiểu sử bảo mật bộ phận thứ nhất được liên kết với bộ phận bảo mật thứ nhất được phân định cho thiết bị truyền thông 304, việc nhận một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai và tiểu sử bảo mật thứ nhất, có thể đủ để tìm ra bộ phận bảo mật mới thỏa mãn một hoặc nhiều khác biệt (tức là, (các) thay đổi mới nhất) bên cạnh các đặc tính khác của tiểu sử bảo mật bộ phận thứ nhất.

Thiết bị mạng 302 còn được tạo cấu hình để xác định bộ phận bảo mật thứ hai đối với thiết bị truyền thông 304 dựa trên thông tin cập nhật bảo mật. Thiết bị mạng 302 được tạo cấu hình để so sánh các thuộc tính bảo mật được liên kết với ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất với các thuộc tính bảo mật tương ứng được liên kết với mỗi tiểu sử trong các tiểu sử bảo mật bộ phận được liên kết với các bộ phận bảo mật. Việc so sánh được thực thi để tìm ra bộ phận so khớp tốt nhất (tức là, bộ phận bảo mật thứ hai trong trường hợp này) đối với thiết bị truyền thông 304 từ trong số các bộ phận bảo mật. Theo phương án thực hiện, thiết bị mạng 302 được tạo cấu hình để sử dụng cả bộ chỉ báo loại tin nhắn (mà chỉ báo, chẳng hạn, yêu cầu theo đòi hỏi để cấp phát lại bộ phận) và tiểu sử bảo mật thứ hai để xác định bộ phận bảo mật thứ hai.

Thiết bị mạng 302 còn được tạo cấu hình để cấp lệnh cho thiết bị truyền thông 304 để gia nhập bộ phận bảo mật thứ hai được xác định. Theo phương án thực hiện, thiết bị mạng 302 còn được tạo cấu hình để cấp, cho thiết bị truyền thông 304, tiểu sử bảo mật bộ phận thứ hai được liên kết với bộ phận bảo mật thứ hai được xác định. Tiểu sử bảo mật bộ phận thứ hai được chia sẻ với thiết bị truyền thông khiến thiết bị truyền thông 304 có thể kiểm chứng quyết định liệu có gia nhập bộ phận bảo mật thứ hai hay không, và do vậy việc chủ động tham gia của thiết bị truyền thông 304 được đảm bảo trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật thứ hai được xác định.

Theo phương án thực hiện, theo cách khác, thiết bị truyền thông 304 còn được tạo cấu hình để thu được (hoặc truy xuất) từ thiết bị mạng 302, danh sách

dịch vụ bảo mật được hỗ trợ bởi thiết bị mạng 302 cho bộ phận bảo mật thứ hai, tiểu sử bảo mật bộ phận thứ hai được liên kết với bộ phận bảo mật thứ hai, hoặc các tiểu sử bảo mật bộ phận của các bộ phận bảo mật khả dụng với thiết bị mạng 302. Thông tin này thu được từ thiết bị mạng 302 khiến thiết bị truyền thông 302 có thể kiểm chứng nếu bộ phận bảo mật thứ hai thích hợp hay không theo ít nhất một thay đổi (tức là, (các) thay đổi mới nhất) trong tiểu sử bảo mật thứ nhất. Nói cách khác, thông tin này (chẳng hạn danh sách các dịch vụ bảo mật, tiểu sử bảo mật bộ phận thứ hai, và các tiểu sử bảo mật bộ phận khả dụng khác) thu được từ thiết bị mạng 302 có thể thương lượng bảo mật và kiểm chứng bảo mật lẫn nhau giữa thiết bị truyền thông 304 và thiết bị mạng 302. Nói cách khác, both thiết bị mạng 302 và thiết bị truyền thông 304 có thể thực thi thương lượng bảo mật, trong đó một bên (chẳng hạn, thiết bị mạng 302) xác định danh sách của các tùy chọn khả dụng để cho phép bên còn lại (chẳng hạn, thiết bị truyền thông 304) lựa chọn tùy chọn so khớp tốt nhất (tức là, đúng bộ phận bảo mật), nhờ đó giảm các sai khớp bộ phận bảo mật, và cải thiện toàn bộ bảo mật mạng và hiệu suất trong quản lý mạng. Do vậy, theo phương án thực hiện, thiết bị truyền thông 304 còn được tạo cấu hình để kiểm chứng quyết định liên quan đến việc gia nhập bộ phận bảo mật thứ hai dựa trên ít nhất đánh giá của tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai.

Thiết bị truyền thông 304 còn được tạo cấu hình để gia nhập bộ phận bảo mật thứ hai thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông, dựa trên lệnh thu được. Thiết bị truyền thông 304 gia nhập bộ phận bảo mật thứ hai nếu kiểm chứng thành công (tức là, thiết bị truyền thông 304 cùng với thiết bị mạng 302 thỏa thuận với nhau rằng bộ phận bảo mật thứ hai là so khớp tốt nhất theo thông tin cập nhật bảo mật). Theo phương án thực hiện, thiết bị truyền thông 304 còn được tạo cấu hình để điều khiển kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông 304 theo tiểu sử bảo mật bộ phận thứ hai thu được được liên kết với bộ phận bảo mật thứ hai, nếu kiểm chứng thành công. Việc kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông 304

có thể được thực thi sau khi kiểm chứng thành công và thiết bị truyền thông 304 gia nhập bộ phận bảo mật thứ hai. Chẳng hạn, thiết bị truyền thông 304 có thể vô hiệu hóa các cập nhật firmware qua mạng truyền thông thứ nhất 306 (chẳng hạn, mạng Wi-Fi) nếu thiết bị mạng 302 (chẳng hạn, bộ định tuyến) không hỗ trợ bộ phận bảo mật dành riêng cho chức năng này do cập nhật firmware qua mạng phẳng (chẳng hạn, mạng truyền thông thứ nhất 306 trong đó tất cả các thiết bị truyền thông được nối qua cùng thiết bị mạng 302) được xem xét là không bảo mật cho thiết bị truyền thông cụ thể, chẳng hạn thiết bị truyền thông 304.

Thiết bị mạng 304 còn được tạo cấu hình để áp dụng chính sách mạng cụ thể được liên kết với bộ phận bảo mật thứ hai đối với thiết bị truyền thông sau khi thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai và rời khỏi bộ phận bảo mật thứ nhất. Chẳng hạn, thiết bị truyền thông 304 có thể là thiết bị IoT. Trong thời gian ghép cặp, thiết bị IoT có thể phải được nối với điện thoại di động (thiết bị truyền thông khác) và riêng URL đám mây cụ thể. Các yêu cầu này có thể được truyền đến thiết bị mạng 302 bởi thiết bị truyền thông 304 dưới dạng thông tin cập nhật bảo mật. Để đáp ứng, thiết bị mạng 302 có thể tạm thời kết nối thiết bị IoT với bộ phận bảo mật dành riêng (hoặc phân định bộ phận bảo mật dành riêng) hỗ trợ cung cấp các thiết bị IoT bởi đám mây cụ thể hoặc điện thoại di động cụ thể, và bộ phận bảo mật dành riêng có chính sách truy nhập dành riêng (chẳng hạn, chính sách mạng cụ thể) được liên kết với chúng.

Theo phương án thực hiện, cả hai hoặc một trong thiết bị mạng 302 hoặc thiết bị truyền thông 304 có thể hỗ trợ chế độ kế thừa và chế độ thương lượng bảo mật. Trong trường hợp trong đó thiết bị mạng cụ thể (chẳng hạn, thiết bị mạng 302) và thiết bị truyền thông cụ thể (chẳng hạn, thiết bị truyền thông 304) không hỗ trợ các hoạt động khác nhau của thiết bị mạng 302 hoặc thiết bị truyền thông 304 để thương lượng bảo mật, như nêu trên, trong các trường hợp này, các thiết bị này có thể tiếp tục hoạt động trong chế độ kế thừa (tức là, như được định nghĩa trong các hệ thống và các phương pháp hiện có để tạo cấu hình mạng). Ngoài ra, trong trường hợp trong đó thương lượng bảo mật, như được mô tả trên đây, trong các hoạt động khác nhau của thiết bị mạng 302 hoặc

thiết bị truyền thông 304 được hỗ trợ, thiết bị mạng cụ thể hoặc thiết bị truyền thông có thể chuyển đổi sang chế độ thương lượng bảo mật. Nói cách khác, thiết bị mạng 302 được bộc lộ và thiết bị truyền thông 304 có thể tương thích ngược và hỗ trợ phân định và gia nhập vào bộ phận bảo mật cụ thể dựa trên khả năng của nó.

Fig.3B là sơ đồ khối minh họa các thành phần lấy làm ví dụ khác nhau của thiết bị mạng, theo phương án thực hiện sáng chế. Fig.3C được mô tả cùng với các phần tử từ Fig.3A. Fig.3B thể hiện thiết bị mạng 302. Thiết bị mạng 302 bao gồm mạch điều khiển 312, giao diện mạng 314, và bộ nhớ 316. Mạch điều khiển 312 có thể được ghép nối truyền thông với giao diện mạng 314 và bộ nhớ 316.

Mạch điều khiển 312 của thiết bị mạng 302 được tạo cấu hình để thu được thông tin cập nhật bảo mật từ thiết bị truyền thông 304. Thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông 304. Theo phương án thực hiện, mạch điều khiển 312 có thể là bộ xử lý đa năng. Theo phương án thực hiện, mạch điều khiển 312 được tạo cấu hình để thực thi các lệnh được lưu trữ trong bộ nhớ 316. Các ví dụ về mạch điều khiển 312 có thể bao gồm, nhưng không bị giới hạn ở bộ vi xử lý, bộ vi điều khiển, bộ xử lý tính toán tập lệnh phức (complex instruction set computing, CISC), bộ xử lý mạch tích hợp ứng dụng cụ thể (application-specific integrated circuit, ASIC), bộ xử lý tập lệnh rút gọn (reduced instruction set, RISC), bộ xử lý từ lệnh rất dài (very long instruction word, VLIW), khối xử lý trung tâm (central processing unit, CPU), máy trạng thái, khối xử lý dữ liệu, và các bộ xử lý hoặc mạch khác. Ngoài ra, mạch điều khiển 312 có thể đề cập đến một hoặc nhiều bộ xử lý cá nhân, thiết bị xử lý, khối xử lý vốn là một phần của máy.

Giao diện mạng 314 có thể bao gồm lôgic thích hợp, mạch, và/hoặc các giao diện có thể được tạo cấu hình để truyền thông với một hoặc nhiều thiết bị bên ngoài, chẳng hạn thiết bị mạng 302 hoặc các thiết bị truyền thông ngang hàng. Các ví dụ về the giao diện mạng 314 có thể bao gồm, nhưng không bị giới hạn ở, bộ thu phát tần số vô tuyến (radio frequency, RF), anten, khối viễn

tin, một hoặc nhiều bộ khuếch đại, một hoặc nhiều bộ dao động, bộ xử lý tín hiệu số (digital signal processor, DSP), chipset bộ mã hóa – bộ giải mã (coder-decoder, CODEC), và/hoặc thẻ mô đun định danh thuê bao (subscriber identity module, SIM). Giao diện mạng 314 có thể truyền thông không dây nhờ sử dụng các giao thức truyền thông hữu tuyến hoặc không dây khác nhau.

Bộ nhớ 316 có thể bao gồm lôgic thích hợp, mạch, và/hoặc giao diện có thể được tạo cấu hình để lưu trữ mã máy và/hoặc các lệnh có ít nhất một đoạn mã có thể thực thi bằng mạch điều khiển 312. Bộ nhớ 316 có thể lưu trữ các tiểu sử bảo mật bộ phận. Các ví dụ về triển khai bộ nhớ 316 có thể bao gồm, nhưng không bị giới hạn ở, bộ nhớ chỉ đọc lập trình được xóa được bằng điện (Electrically Erasable Programmable Read-Only Memory, EEPROM), bộ nhớ truy nhập ngẫu nhiên (Random Access Memory, RAM), bộ nhớ chỉ đọc (Read Only Memory, ROM), ổ đĩa cứng (Hard Disk Drive, HDD), bộ nhớ nhanh, thẻ nhớ số bảo mật (Secure Digital, SD), ổ trạng thái rắn (Solid-State Drive, SSD), vật lưu trữ máy tính đọc được, và/hoặc bộ nhớ cache CPU. Bộ nhớ 316 có thể lưu trữ hệ điều hành và/hoặc các sản phẩm chương trình khác để vận hành thiết bị mạng 402. Vật lưu trữ máy tính đọc được để cung cấp bộ nhớ bất biến có thể bao gồm, nhưng không bị giới hạn ở, thiết bị lưu trữ điện tử, thiết bị lưu trữ từ tính, thiết bị lưu trữ quang, thiết bị lưu trữ điện từ, thiết bị lưu trữ bán dẫn, hoặc tổ hợp thích hợp bất kỳ trong các thiết bị nêu trên.

Fig.3C là sơ đồ khối minh họa các thành phần lấy làm ví dụ khác nhau của thiết bị truyền thông, theo phương án thực hiện sáng chế. Fig.3C được mô tả cùng với các phần tử từ Fig.1, Fig.2, Fig.3A, và Fig.3B. Fig.3C thể hiện thiết bị truyền thông 304. Thiết bị truyền thông 304 bao gồm mạch điều khiển 318, giao diện mạng 320, bộ phận nhập/xuất (input/output, I/O) 322, và bộ nhớ 324. Mạch điều khiển 318 có thể được ghép nối truyền thông với giao diện mạng 320, bộ phận I/O 322, và bộ nhớ 324.

Mạch điều khiển 318 của thiết bị truyền thông 304 được tạo cấu hình để cấp thông tin cập nhật bảo mật cho thiết bị mạng 302. Theo phương án thực hiện, mạch điều khiển 318 được tạo cấu hình để thực thi các lệnh được lưu trữ trong bộ nhớ 324. Các ví dụ về mạch điều khiển 318 giống như ví dụ về mạch

điều khiển 312 (Fig.3B). Tương tự, các ví dụ về việc triển khai giao diện mạng 320 và bộ nhớ 324 lần lượt giống như việc triển khai giao diện mạng 314 và bộ nhớ 316 trên Fig.3B.

Bộ phận I/O 322 là các bộ phận nhập và xuất có thể nhận đầu vào từ người dùng và tạo đầu ra cho người dùng. Bộ phận I/O 322 có thể được ghép nối truyền thông với mạch điều khiển 318. Các ví dụ về các bộ phận nhập liệu có thể bao gồm, nhưng không bị giới hạn ở, màn hình cảm ứng, chẳng hạn màn hình cảm ứng của thiết bị hiển thị, micrô, bộ cảm biến chuyển động, bộ cảm biến ánh sáng, khối đầu vào phần cứng dành riêng (chẳng hạn, nút nhấn hoặc bàn phím), và trạm nối. Các ví dụ về bộ phận xuất bao gồm bộ phận hiển thị và loa. Các ví dụ về bộ phận hiển thị bao gồm, nhưng không bị giới hạn ở màn hình hiển thị, hiển thị kính thông minh, hiển thị theo hình chiếu, hiển thị dựa trên thực tế ảo, hoặc màn hiển thị khác.

Fig.4 là sơ đồ minh họa các thành phần chức năng lấy làm ví dụ khác nhau của thiết bị mạng và thiết bị truyền thông để thực thi thương lượng bảo mật để cấu hình mạng, theo phương án thực hiện sáng chế. Fig.4 được mô tả cùng với các phần tử từ Fig.1, Fig.2, và Fig.3A đến Fig.3C. Fig.4 thể hiện thiết bị mạng 302 và thiết bị truyền thông 304. Ngoài ra còn thể hiện bộ thương lượng bảo mật 402, bộ quản lý bộ phận bảo mật 404, bộ điều khiển luồng 406, bộ chuyển mạch gói 408, và giao diện mạng 314 trong thiết bị mạng 302. Bộ phận thương lượng bảo mật 402 bao gồm bộ thương lượng bảo mật 402a, bộ đăng ký thiết bị 402b, bộ tạo tiểu sử bảo mật 402c, và bộ quản lý chính sách 402d. Ngoài ra, còn thể hiện bộ thương lượng bảo mật 410, bộ thực thi chính sách 412, chức năng ứng dụng 414, trạng thái hệ thống 416, và giao diện mạng 320 trong thiết bị truyền thông 304. Cũng thể hiện bộ phận thương lượng 418, bộ phận bảo mật thứ nhất 420, và bộ phận bảo mật thứ hai 422.

Các thành phần chức năng lấy làm ví dụ khác nhau của thiết bị mạng 302 và thiết bị truyền thông 304 có thể được triển khai dưới dạng các môđun phần mềm, các môđun phần cứng, hoặc kết hợp của phần mềm và các linh kiện phần cứng (chẳng hạn, mã thực thi được, lôgic, các giao diện, hoặc các mạch). Theo phương án thực hiện, các hoạt động hoặc các chức năng được thực hiện bởi các

thành phần chức năng này (chẳng hạn, bộ phận thương lượng bảo mật 402, bộ quản lý bộ phận bảo mật 404, bộ điều khiển luồng 406, và bộ chuyển mạch gói 408) của thiết bị mạng 302 có thể được quản lý và vận hành tập trung dưới sự điều khiển của mạch điều khiển 312 (Fig.3B) của thiết bị mạng 302. Theo phương án thực hiện khác, tất cả các chức năng hoặc các hoạt động của các thành phần chức năng khác nhau của thiết bị mạng 302 có thể được thực hiện bằng mạch điều khiển 312 của thiết bị mạng 302. Tương tự, các thành phần chức năng khác nhau (chẳng hạn bộ thương lượng bảo mật 410, bộ thực hiện chính sách 412, chức năng ứng dụng 414, và trạng thái hệ thống 416) của thiết bị truyền thông 304 có thể được vận hành theo điều khiển của mạch điều khiển 318 (Fig.3C) của thiết bị truyền thông 304.

Bộ phận thương lượng bảo mật 402 của thiết bị mạng 302 hỗ trợ thương lượng bảo mật với các thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304. Bộ phận thương lượng bảo mật 402 được tạo cấu hình để truyền thông với các thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304, theo bộ phận thương lượng 418. Bộ phận thương lượng bảo mật 402 bao gồm bộ thương lượng bảo mật 402a.

Bộ thương lượng bảo mật 402a được tạo cấu hình để thu được (hoặc cảm nhận) thông tin (chẳng hạn, qua giao diện mạng 314) liên quan đến mỗi thiết bị trong các thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304, được ghép nối truyền thông với thiết bị mạng 302. Bộ thương lượng bảo mật 402a còn được tạo cấu hình để cung cấp thông tin được cảm nhận (tức là, thông tin thu được từ thiết bị truyền thông 304) đến các thành phần chức năng khác nhau, chẳng hạn bộ đăng ký thiết bị 402b, bộ tạo tiểu sử bảo mật 402c, bộ quản lý chính sách 402d, bộ điều khiển luồng 406, và bộ chuyển mạch gói 408, để xác định bộ phận bảo mật cụ thể từ các bộ phận bảo mật thích hợp đối với thiết bị truyền thông 304. Trong ví dụ, bộ thương lượng bảo mật 402a còn được tạo cấu hình để sử dụng thông tin được truy xuất từ các API cụ thể (chẳng hạn, các API thiết bị mở), sử dụng các giao thức lớp ứng dụng (chẳng hạn, giao thức quản lý mạng đơn giản (simple network management protocol, SNMP)), các dịch vụ đám mây cụ thể (chẳng hạn, đặc tả mô tả sử dụng của nhà sản xuất

(manufacturer usage description, MUD)) và/hoặc sử dụng phân tích truyền thông bởi thiết bị truyền thông 304, để xác định đúng bộ phận bảo mật (chẳng hạn, bộ phận bảo mật thứ nhất hoặc bộ phận bảo mật thứ hai) đối với thiết bị truyền thông 304. Một cách có lợi, bộ thương lượng bảo mật 402a hỗ trợ các chức năng khác nhau, chẳng hạn cung cấp cho các thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304 (hoặc quảng cáo hoặc công bố trên mạng), danh sách dịch vụ bảo mật được hỗ trợ bởi thiết bị mạng 302, và các tiểu sử bảo mật bộ phận của các bộ phận bảo mật khả dụng với thiết bị mạng 302. Bộ thương lượng bảo mật 402a còn phục vụ các yêu cầu liên quan đến yêu cầu thông tin, yêu cầu cấp phát lại bộ phận, yêu cầu chia sẻ tiểu sử bộ phận, hoặc yêu cầu cập nhật tiểu sử, và tương tự, khi được nhận từ các thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304.

Trong ví dụ, bộ đăng ký thiết bị 402b có thể là cơ sở dữ liệu trong đó danh sách của các thiết bị truyền thông được đăng ký ở thiết bị mạng 302 được duy trì. Chẳng hạn, danh sách hiện tại của các thiết bị truyền thông đã gia nhập bộ phận bảo mật cụ thể từ các bộ phận bảo mật, có thể được đăng ký trong bộ đăng ký thiết bị 402b. Một cách tùy chọn, bộ đăng ký thiết bị 402b có thể cũng duy trì dữ liệu lịch sử (chẳng hạn, các nhãn thời gian và các định danh thiết bị tương ứng) liên quan đến việc gia nhập và rời đi của bộ phận bảo mật cụ thể bởi thiết bị truyền thông trong các thiết bị truyền thông, chẳng hạn thiết bị truyền thông 304.

Bộ tạo tiểu sử bảo mật 402c được tạo cấu hình để so sánh các thuộc tính bảo mật đã liên kết tiểu sử bảo mật cụ thể của thiết bị truyền thông (chẳng hạn thiết bị truyền thông 304) với các thuộc tính bảo mật tương ứng được liên kết với mỗi tiểu sử trong các tiểu sử bảo mật bộ phận được liên kết với các bộ phận bảo mật. Bộ tạo tiểu sử bảo mật 402c được ghép nối truyền thông với bộ quản lý bộ phận 404a qua bộ điều khiển luồng 406.

Bộ quản lý chính sách 402d được tạo cấu hình để quản lý các chính sách mạng khác nhau được liên kết với các bộ phận bảo mật khác nhau. Ngoài ra, bộ quản lý chính sách 402d được tạo cấu hình để áp dụng chính sách mạng cụ thể được liên kết với bộ phận bảo mật cụ thể đối với thiết bị truyền thông cụ thể

(chẳng hạn, thiết bị truyền thông 304) sau khi thiết bị truyền thông gia nhập bộ phận bảo mật cụ thể.

Bộ quản lý bộ phận bảo mật 404 hỗ trợ quản lý các tiểu sử bảo mật bộ phận của các bộ phận bảo mật ở thiết bị mạng 302. Bộ quản lý bộ phận bảo mật 404 bao gồm bộ quản lý bộ phận 404a, và bộ xây dựng mạng 404b. Bộ quản lý bộ phận 404a có thể chịu trách nhiệm tạo và quản lý các tiểu sử bảo mật bộ phận, và việc chia sẻ tiếp các tiểu sử bảo mật bộ phận này theo các yêu cầu được nhận từ các thiết bị truyền thông (chẳng hạn thiết bị truyền thông 304).

Bộ điều khiển luồng 406 chịu trách nhiệm quản lý luồng thông tin và các lệnh đến và từ thiết bị mạng 302 cho hoạt động gia nhập lần đầu tiên và các yêu cầu cấp phát lại bộ phận theo yêu cầu từ các thiết bị truyền thông (chẳng hạn, thiết bị truyền thông 304).

Bộ chuyển mạch gói 408 có thể truyền dữ liệu giữa thiết bị mạng 302 và mỗi thiết bị trong các thiết bị truyền thông (chẳng hạn, thiết bị truyền thông 304) ở dạng gói dữ liệu trên bộ phận bảo mật được cấp phát (chẳng hạn, bộ phận bảo mật thứ nhất 420 hoặc bộ phận bảo mật thứ hai 422). Mỗi gói dữ liệu có thể bao gồm các chi tiết khác nhau, chẳng hạn địa chỉ IP nguồn, địa chỉ IP đích và dữ liệu duy nhất, và các định danh gói. Khi thiết bị truyền thông 304 gia nhập bộ phận bảo mật thứ hai 422 và rời khỏi bộ phận bảo mật thứ nhất 420, bộ chuyển mạch gói 408 được tạo cấu hình để chuyển đổi lưu lượng dữ liệu và truyền thông liên quan chỉ trên bộ phận bảo mật thứ hai 422.

Bộ thương lượng bảo mật 410 của thiết bị truyền thông 304 hỗ trợ thương lượng bảo mật với thiết bị mạng 302, chẳng hạn, trên bộ phận thương lượng 418. Một cách có lợi, bộ thương lượng bảo mật 410 hỗ trợ các chức năng khác nhau, chẳng hạn cung cấp tiểu sử bảo mật thứ nhất (tức là, tiểu sử bảo mật thiết bị) cho thiết bị mạng 302 (hoặc quảng cáo hoặc công bố trên mạng sao cho thiết bị mạng 302 có thể thu được tiểu sử bảo mật thứ nhất được công bố). Bộ thương lượng bảo mật 410 được tạo cấu hình để truyền thông các yêu cầu khác nhau, chẳng hạn yêu cầu thông tin, yêu cầu cấp phát lại bộ phận, yêu cầu chia sẻ tiểu sử bộ phận, hoặc yêu cầu cập nhật tiểu sử, cho thiết bị mạng 302. Bộ thương lượng bảo mật 410 cập nhật thiết bị mạng 302 nếu có bất kỳ thay đổi

trong các yêu cầu bảo mật (chẳng hạn, thông tin cập nhật bảo mật chỉ báo các thay đổi mới nhất trong tiểu sử bảo mật thứ nhất) của thiết bị truyền thông 304. Bộ thương lượng bảo mật 410 còn được tạo cấu hình để truy xuất danh sách các dịch vụ bảo mật được hỗ trợ bởi thiết bị mạng 302, tiểu sử bảo mật bộ phận của bộ phận bảo mật mới (chẳng hạn, bộ phận bảo mật thứ hai 422) được phân định cho thiết bị truyền thông 304, và/hoặc các tiểu sử bảo mật bộ phận của các bộ phận bảo mật khả dụng với thiết bị mạng 302. Bộ thương lượng bảo mật 410 đảm bảo việc chủ động tham gia của thiết bị truyền thông 304 trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật cụ thể được xác định (hoặc được cấp phát) bởi thiết bị mạng 302. Bộ thương lượng bảo mật 410 được tạo cấu hình để thông báo bộ thực hiện chính sách 412 để thực thi chức năng thực hiện chính sách cục bộ có điều chỉnh chức năng được đề xuất theo tiểu sử bảo mật bộ phận của bộ phận bảo mật (chẳng hạn bộ phận bảo mật thứ nhất 420 hoặc bộ phận bảo mật thứ hai 422) được gia nhập bởi thiết bị truyền thông 304.

Bộ thực hiện chính sách 412 chịu trách nhiệm kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông 304 theo tiểu sử bảo mật bộ phận của bộ phận bảo mật (chẳng hạn, bộ phận bảo mật thứ nhất 420 hoặc bộ phận bảo mật thứ hai 422) được gia nhập bởi thiết bị truyền thông 304.

Chức năng ứng dụng 414 được tạo cấu hình để dò thấy thay đổi trong trạng thái ứng dụng của một hoặc nhiều ứng dụng, hệ điều hành và dữ liệu liên kết, hoặc trạng thái phần cứng của thiết bị truyền thông 304. Chẳng hạn, bất kỳ thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông 304 hoặc thay đổi trong môi trường mạng của thiết bị truyền thông 304 mà có thể ảnh hưởng bảo mật của thiết bị truyền thông 304, được dò thấy. (Các) thay đổi được dò thấy này được thông báo đến trạng thái hệ thống 416.

Trạng thái hệ thống 416 có thể đề cập đến máy ghi (hoặc cơ sở dữ liệu) ghi lại (các) thay đổi được dò thấy và thông báo bởi chức năng ứng dụng 414. Tiểu sử bảo mật thứ nhất được cập nhật thành tiểu sử bảo mật thứ hai dựa trên một hoặc nhiều thay đổi của trạng thái hoạt động của thiết bị hoặc môi trường mạng của thiết bị truyền thông 304. Sau đó, bộ thương lượng bảo mật 410 cập nhật

thiết bị mạng 302 về (các) thay đổi này trong các yêu cầu bảo mật dưới dạng thông tin cập nhật bảo mật chỉ báo các thay đổi mới nhất trong tiểu sử bảo mật thứ nhất của thiết bị truyền thông 304.

Fig.5 minh họa kịch bản 500 lấy làm ví dụ mô tả nguyên lý làm việc thương lượng bảo mật để tạo cấu hình mạng, theo phương án thực hiện sáng chế. Fig.5 được mô tả cùng với các phần tử từ Fig.1, Fig.2, Fig.3A đến Fig.3C, và Fig.4. Fig.5 thể hiện kịch bản lấy làm ví dụ 500 mô tả tiểu sử bảo mật thứ nhất 502 và tiểu sử bảo mật thứ hai 504 của thiết bị truyền thông 304. Ngoài ra còn thể hiện tiểu sử bảo mật bộ phận thứ nhất 504 và tiểu sử bảo mật bộ phận thứ hai 506 của thiết bị mạng 302 (Fig.3A). Cũng thể hiện bộ phận bảo mật thứ nhất 420 và bộ phận bảo mật thứ hai 422.

Theo kịch bản lấy làm ví dụ 500, các định nghĩa tiểu sử của các tiểu sử bảo mật khác nhau (chẳng hạn, tiểu sử bảo mật thứ nhất 502, tiểu sử bảo mật thứ hai 504, tiểu sử bảo mật bộ phận thứ nhất 504, và tiểu sử bảo mật bộ phận thứ hai 506) được biểu diễn bằng các vectơ của hàm (chẳng hạn, các đặc tính, các dịch vụ, hoặc yêu cầu bảo mật), trong đó "V" chỉ báo "phải được hỗ trợ", "X" chỉ báo "phải bị vô hiệu hóa", và hộp trống chỉ báo tư thế trung gian trong đó bất kỳ trạng thái nào cũng được.

Như được thể hiện, thiết bị truyền thông 304 có thể bao gồm tiểu sử bảo mật thứ nhất 502 chỉ báo trạng thái hoạt động của thiết bị thứ nhất của thiết bị truyền thông 304. Như được thể hiện, trong tiểu sử bảo mật thứ nhất 502, có các khe bao gồm "V", hộp trống, hoặc "X". Thiết bị truyền thông 304 có tiểu sử bảo mật thứ nhất 502 trong trạng thái hoạt động của thiết bị thứ nhất được phân định cho bộ phận bảo mật thứ nhất 420. Bộ phận bảo mật thứ nhất 420 được liên kết với tiểu sử bảo mật bộ phận thứ nhất 504 thích hợp đối với thiết bị truyền thông 304 theo tiểu sử bảo mật thứ nhất 502 của thiết bị truyền thông 304. Chẳng hạn, khe 510A trong tiểu sử bảo mật thứ nhất 502 là hộp trống không thiết lập bất kỳ yêu cầu bảo mật nào đối với tính năng cụ thể (chẳng hạn, FTP tải lên URL cụ thể) của khe 510A. Do vậy, thiết bị truyền thông 304 được bảo mật đầy đủ khi được nối với bộ phận bảo mật thứ nhất 422 được liên kết với tiểu sử bảo mật bộ phận thứ nhất 504, trong đó đặc tính cụ thể (chẳng hạn,

FTP tải lên URL cụ thể) được phép và được hỗ trợ (được ký hiệu là "V" trong khe tương ứng 510B). Tuy nhiên, trạng thái hoạt động của thiết bị của thiết bị truyền thông 304 có thể thay đổi từ trạng thái hoạt động của thiết bị thứ nhất sang trạng thái hoạt động của thiết bị thứ hai. Sau đó, tiểu sử bảo mật thứ nhất 502 được cập nhật thành tiểu sử bảo mật thứ hai 504 để phản ánh thay đổi trong trạng thái hoạt động của thiết bị. Chẳng hạn, yêu cầu mới có thể liên quan đến "sao chép các ủy nhiệm người dùng", và do vậy, đặc tính cụ thể trong khe 510A trong tiểu sử bảo mật thứ hai 504 có thể bắt đầu va chạm (tức là, xung đột) với khe tương ứng 510B của tiểu sử bảo mật bộ phận thứ nhất 504. Yêu cầu mới chính là đặc tính cụ thể (hoặc chức năng) phải được vô hiệu hóa trong chu kỳ sao dự phòng (chẳng hạn, trong khi FTP tải lên URL cụ thể). Thiết bị truyền thông 304 được tạo cấu hình để truyền yêu cầu cấp phát lại bộ phận bảo mật đến thiết bị mạng 302. Thiết bị truyền thông 304 còn cấp tiểu sử bảo mật thứ hai 504 cho thiết bị mạng 302 cùng với yêu cầu sau khi dò thấy xung đột tiểu sử (và trước khi bắt đầu sao dự phòng thực sự ở thiết bị truyền thông 304 sử dụng URL cụ thể). Đáp lại yêu cầu được nhận và tiểu sử bảo mật thứ hai 504, thiết bị mạng 302 được tạo cấu hình để xác định bộ phận bảo mật thứ hai 422 do sơ khớp tốt nhất thỏa mãn yêu cầu mới (tức là, thay đổi mới nhất). Chẳng hạn, tiểu sử bảo mật bộ phận thứ hai 506 được liên kết với bộ phận bảo mật thứ hai 422 có đặc tính cụ thể bị vô hiệu hóa (chẳng hạn, "sao dự phòng các ủy nhiệm người dùng" bị vô hiệu hóa cho chu kỳ sao dự phòng) ở khe 510B. Do vậy, trong trường hợp này, bảo mật được tăng bền khi thiết bị truyền thông gia nhập bộ phận bảo mật thứ hai 422.

Fig.6 minh họa kịch bản lấy làm ví dụ 600 mô tả thực thi thương lượng bảo mật để cấu hình mạng cho các thiết bị truyền thông khác nhau, theo phương án thực hiện sáng chế. Fig.6 được mô tả cùng với các phần tử từ Fig.1, Fig.2, Fig.3A đến Fig.3C, Fig.4, và Fig.5. Fig.6 thể hiện kịch bản lấy làm ví dụ 600 bao gồm thiết bị cổng nối 602, nhóm thiết bị không tin cậy 604, nhóm thiết bị tin cậy 606, và nhóm thiết bị IoT 608. Ngoài ra còn thể hiện bộ phận bảo mật thứ nhất 610, bộ phận bảo mật thứ hai 612, và bộ phận bảo mật thứ ba 614, mạng truyền thông 616, đường kết nối mạng thay thế 618, và tập hợp kết nối

mạng 620 từ bộ điều khiển IoT 622 trong nhóm thiết bị IoT 608 đến các thiết bị IoT ngang hàng.

Theo kịch bản lấy làm ví dụ 600, thiết bị cổng nối 602 tương ứng với thiết bị mạng 302 (Fig.3A). Mỗi nhóm trong nhóm thiết bị không tin cậy 604, nhóm thiết bị tin cậy 606, và nhóm thiết bị IoT 608 tương ứng với thiết bị truyền thông 304 (Fig.3A). Mỗi nhóm trong nhóm thiết bị không tin cậy 604, nhóm thiết bị tin cậy 606, và nhóm thiết bị IoT 608 có thể được nối trực tiếp với thiết bị cổng nối 602 qua mạng W-Fi, và có thể truy nhập các tài nguyên mạng của mạng truyền thông 616 (chẳng hạn, mạng Internet) qua thiết bị cổng nối 602. Các thiết bị IoT cụ thể, chẳng hạn, các thiết bị IoT 624, có thể không được nối trực tiếp với thiết bị cổng nối 602, và có thể được ghép nối truyền thông với thiết bị IoT khác, chẳng hạn bộ điều khiển IoT 622 qua tập hợp kết nối mạng 620.

Thông thường, trong các hệ thống và các phương pháp đã biết, các truyền thông qua tập hợp kết nối mạng 620 giữa bộ điều khiển IoT 622 và các thiết bị IoT 624, có thể vô hình với thiết bị cổng nối đã biết. Nói cách khác, thiết bị cổng nối đã biết có thể không nhận thức về các truyền thông này, có thể có các phép bao hàm bảo mật bất lợi. Ngoài ra, các thiết bị IoT cụ thể, chẳng hạn bộ điều khiển IoT 622 có thể bỏ qua thiết bị cổng nối 602, và trực tiếp truy nhập mạng truyền thông 616 (tức là, mạng Internet) nhờ sử dụng đường kết nối mạng tùy chọn 618 (chẳng hạn, mạng tế bào). Trong các hệ thống và các phương pháp đã biết, thiết bị cổng nối đã biết cũng có thể không nhận thức được các phiên truyền thông này được thực hiện qua đường kết nối mạng tùy chọn 618, có thể có các ngụ ý bảo mật xấu. Ngược với các hệ thống và các phương pháp đã biết, các phương pháp và các thiết bị được bộc lộ (chẳng hạn, thiết bị cổng nối 602) bắt được các phiên truyền thông không bị lộ này nhờ sử dụng tiểu sử bảo mật (chẳng hạn, tiểu sử bảo mật thứ nhất) của mỗi thiết bị truyền thông (chẳng hạn, mỗi nhóm trong nhóm thiết bị không tin cậy 604, nhóm thiết bị tin cậy 606, và nhóm thiết bị IoT 608a có tiểu sử bảo mật riêng, được gọi là tiểu sử bảo mật thứ nhất). Tiểu sử bảo mật thứ nhất này được cấp bởi mỗi nhóm trong nhóm thiết bị không tin cậy 604, nhóm thiết bị tin cậy 606,

và nhóm thiết bị IoT 608, có thể đánh giá tăng cường các khả năng bảo mật và các yêu cầu bảo mật của các thiết bị riêng rẽ bởi thiết bị cổng nối 602. Chẳng hạn, các đặc tính bảo mật cụ thể (hoặc thuộc tính bảo mật) của mỗi thiết bị truyền thông bên cạnh đó có thể vẫn không được dò thấy (tức là, không bị lộ) qua kênh truyền thông Wi-Fi thông thường (chẳng hạn, sử dụng chức năng tự phát hiện) bởi thiết bị cổng nối 602, được dễ dò thấy và chính xác nhờ sử dụng tiểu sử bảo mật thứ nhất. Do vậy, tiểu sử bảo mật thứ nhất khiến thiết bị cổng nối 602 có thể xác định bộ phận bảo mật so khớp tốt nhất từ trong số các bộ phận bảo mật để phân định cho các thiết bị truyền thông tương ứng, nhờ đó bảo mật đầy đủ. Chẳng hạn, nhóm thiết bị không tin cậy 604 có thể là các thiết bị khách (chẳng hạn, có loại thiết bị chưa biết, nhà sản xuất không được hỗ trợ, hoặc các thiết bị của nhà cung cấp chưa biết có thể hoạt động theo cách không dự báo được), có thể được phân định bộ phận bảo mật dành riêng, chẳng hạn bộ phận bảo mật thứ nhất 610, trong đó bảo mật được tăng cường tương đối hơn (tức là, truy nhập bị giới hạn) so với nhóm thiết bị tin cậy 606. Tương tự, dựa trên tiểu sử bảo mật thứ nhất thu được từ mỗi thiết bị truyền thông, thiết bị cổng nối 602 còn được tạo cấu hình để xác định bộ phận bảo mật thứ hai 612 cho nhóm thiết bị tin cậy 606, và bộ phận bảo mật thứ ba 614 cho nhóm thiết bị IoT 608. Trong các trường hợp trong đó có thay đổi trong trạng thái hoạt động của thiết bị hoặc môi trường mạng của một hoặc nhiều thiết bị truyền thông (chẳng hạn, một hoặc nhiều trong số nhóm thiết bị không tin cậy 604, nhóm thiết bị tin cậy 606, và nhóm thiết bị IoT 608), thông tin cập nhật bảo mật tương ứng với các thiết bị truyền thông này được chủ động cấp cho thiết bị cổng nối 602. Các cập nhật xuất phát từ thiết bị truyền thông (tức là thông tin cập nhật bảo mật) có thể tham gia chủ động của mỗi thiết bị truyền thông được kết nối trong các quyết định liên quan đến việc liên kết với bộ phận bảo mật. do thông tin cập nhật bảo mật được chủ động chia sẻ bởi mỗi thiết bị truyền thông, thiết bị cổng nối 602 có thể xác định đúng bộ phận bảo mật thực hiện thay đổi mới nhất trong tiểu sử bảo mật thứ nhất của các thiết bị truyền thông tương ứng theo thời gian thực hoặc gần thời gian thực. Do vậy, các cơ hội sai khớp bộ phận bảo mật được giảm đáng kể, nhờ đó giảm rủi ro của các lỗ hổng bảo mật

trong mỗi thiết bị truyền thông tham gia và cải thiện toàn bộ bảo mật mạng và hiệu suất trong quản lý mạng.

Các sửa đổi với các phương án thực hiện sáng chế được mô tả trên đây là khả khi mà không xa rời phạm vi của sáng chế như được định nghĩa bởi các điểm yêu cầu bảo hộ đi kèm. Các cụm từ, chẳng hạn, "bao gồm", "đưa vào", "có", "là" được sử dụng để mô tả và bảo hộ sáng chế sẽ được hiểu theo nghĩa không loại trừ, tức là cho phép các mục, các thành phần hoặc các phần tử không được mô tả tường minh cũng xuất hiện. Tham chiếu tới số ít cũng được hiểu là liên quan đến số nhiều. Từ "lấy làm ví dụ" được sử dụng ở đây nghĩa là "dùng làm ví dụ, thực thể hoặc minh họa". Phương án thực hiện bất kỳ được mô tả như là "lấy làm ví dụ" không nhất thiết được hiểu như là được ưu tiên hoặc có lợi so với các phương án thực hiện khác và/hoặc loại trừ việc đưa các dấu hiệu từ các phương án thực hiện khác. Từ "một cách tùy chọn" được sử dụng ở đây nghĩa là "được bố trí theo một số phương án thực hiện và không được nêu theo các phương án thực hiện khác". Cần hiểu rằng các dấu hiệu cụ thể của sáng chế, được mô tả cho dễ dáng trong ngữ cảnh của các phương án thực hiện riêng rẽ, cũng có thể được nêu kết hợp theo một phương án thực hiện. Ngược lại, các dấu hiệu khác của sáng chế được mô tả vắn tắt trong ngữ cảnh của một phương án thực hiện, cũng có thể được nêu riêng rẽ hoặc kết hợp thích hợp bất kỳ hoặc thích hợp theo phương án thực hiện được mô tả khác bất kỳ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp (100) thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị mạng (302), phương pháp bao gồm các bước:

thu được, bởi thiết bị mạng (302), thông tin cập nhật bảo mật từ thiết bị truyền thông (304) được phân định cho bộ phận bảo mật thứ nhất (420, 610), bộ phận bảo mật thứ nhất (420, 610) được liên kết với tiểu sử bảo mật bộ phận thứ nhất (506), trong đó thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất (502) của thiết bị truyền thông (304),

xác định, bởi thiết bị mạng (302), bộ phận bảo mật thứ hai (422, 612) đối với thiết bị truyền thông (304) dựa trên thông tin cập nhật bảo mật; và

cấp, bởi thiết bị mạng (302), lệnh cho thiết bị truyền thông (304) để gia nhập bộ phận bảo mật thứ hai được xác định (422, 612).

2. Phương pháp (100) theo điểm 1, trong đó phương pháp còn bao gồm bước cung cấp, bởi thiết bị mạng (302), cho thiết bị truyền thông (304), tiểu sử bảo mật bộ phận thứ hai (508) được liên kết với bộ phận bảo mật thứ hai được xác định (422, 612), trong đó tiểu sử bảo mật bộ phận thứ hai (508) được sử dụng bởi thiết bị truyền thông (304) để: kiểm chứng quyết định gia nhập bộ phận bảo mật thứ hai (422, 612); và điều khiển, dựa trên kiểm chứng, kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông (304) theo tiểu sử bảo mật bộ phận thứ hai (508).

3. Phương pháp (100) theo điểm 1 hoặc 2, trong đó hoạt động thu thập thông tin cập nhật bảo mật bởi thiết bị mạng (302) dựa trên thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông (304) hoặc thay đổi trong môi trường mạng của thiết bị truyền thông (304).

4. Phương pháp (100) theo điểm bất kỳ trong số các điểm nêu trên, trong đó việc xác định bộ phận bảo mật thứ hai (422, 612) đối với thiết bị truyền thông (304) bao gồm bước so sánh các thuộc tính bảo mật được liên kết với ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất (502) với các thuộc

tính bảo mật tương ứng được liên kết với mỗi tiểu sử trong các tiểu sử bảo mật bộ phận được liên kết với các bộ phận bảo mật.

5. Phương pháp (100) theo điểm bất kỳ trong số các điểm nêu trên, trong đó phương pháp còn bao gồm bước áp dụng chính sách mạng cụ thể được liên kết với bộ phận bảo mật thứ hai (422, 612) đối với thiết bị truyền thông (304) sau khi thiết bị truyền thông (304) gia nhập bộ phận bảo mật thứ hai (422, 612) và rời khỏi bộ phận bảo mật thứ nhất (420, 610).

6. Phương pháp (100) theo điểm bất kỳ trong số các điểm nêu trên, trong đó tiểu sử bảo mật thứ nhất (502) bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông (304), hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông (304), và trong đó tiểu sử bảo mật thứ nhất (502) được cập nhật bởi thiết bị truyền thông (304) thành tiểu sử bảo mật thứ hai dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông (304) hoặc thay đổi trong môi trường mạng của thiết bị truyền thông (304).

7. Phương pháp (100) theo điểm 6, trong đó thông tin cập nhật bảo mật tương ứng với ít nhất một trong: tiểu sử bảo mật thứ hai (504) hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai (504) và tiểu sử bảo mật thứ nhất (502), và trong đó tiểu sử bảo mật thứ hai (504) bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông (304), yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ trong bộ phận bảo mật thứ nhất (420, 610) được phân định cho thiết bị truyền thông (304), hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông (304).

8. Phương pháp (100) theo điểm 7, trong đó việc xác định bộ phận bảo mật thứ hai (422, 612) đối với thiết bị truyền thông (304) bao gồm việc sử dụng bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ hai.

9. Phương pháp (100) theo điểm bất kỳ trong số các điểm nêu trên, trong đó thiết bị truyền thông (304) được phân định cho bộ phận bảo mật thứ nhất (420, 610) dựa trên hoạt động gia nhập lần đầu tiên giữa thiết bị mạng (302) và thiết bị truyền thông (304), và trong đó hoạt động gia nhập lần đầu tiên bao gồm các bước:

thu được, bởi thiết bị mạng (302), tiểu sử bảo mật thứ nhất (502) từ thiết bị truyền thông (304) theo bộ phận thương lượng (418) khi thiết bị truyền thông (304) ở trạng thái không được phân định đến bộ phận bảo mật cụ thể, và trong đó tiểu sử bảo mật thứ nhất (502) chỉ báo các khả năng của thiết bị và các yêu cầu bảo mật của thiết bị truyền thông (304) ở trạng thái không được phân định;

xác định, bởi thiết bị mạng (302), bộ phận bảo mật thứ nhất (420, 610) từ các bộ phận bảo mật để phân định cho thiết bị truyền thông (304) dựa trên tiểu sử bảo mật thứ nhất thu được (502); và

cấp lệnh cho thiết bị truyền thông (304) để gia nhập bộ phận bảo mật thứ nhất (420, 610), trong đó lệnh thông báo thiết bị truyền thông (304) về bộ phận bảo mật thứ nhất được xác định (420, 610) liên quan đến các khả năng thiết bị và các yêu cầu bảo mật của thiết bị truyền thông (304).

10. Phương pháp (200) thực hiện thương lượng bảo mật cho cấu hình mạng ở thiết bị truyền thông (304), trong đó phương pháp bao gồm các bước:

cấp, bởi thiết bị truyền thông (304), thông tin cập nhật bảo mật cho thiết bị mạng (302), thiết bị truyền thông (304) được phân định cho bộ phận bảo mật thứ nhất (420, 610) được liên kết với tiểu sử bảo mật bộ phận thứ nhất (506), trong đó thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất (502) của thiết bị truyền thông (304);

thu được, bởi thiết bị truyền thông (304), lệnh từ thiết bị mạng (302) để gia nhập bộ phận bảo mật thứ hai (422, 612); và

gia nhập, bởi thiết bị truyền thông (304), bộ phận bảo mật thứ hai (422, 612) thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất (502) của thiết bị truyền thông (304), dựa trên lệnh thu được.

11. Phương pháp (200) theo điểm 10, trong đó thông tin cập nhật bảo mật được cấp bởi thiết bị truyền thông (304) cho thiết bị mạng (302) dựa trên thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông (304) hoặc thay đổi trong môi trường mạng của thiết bị truyền thông (304).

12. Phương pháp (200) theo điểm 10 hoặc 11, trong đó tiểu sử bảo mật thứ nhất (502) bao gồm một hoặc nhiều: các thuộc tính thiết bị, trạng thái hoạt động của thiết bị, môi trường mạng của thiết bị truyền thông (304), hoặc yêu cầu truy nhập một hoặc nhiều dịch vụ ở thiết bị truyền thông (304).

13. Phương pháp (200) theo điểm bất kỳ trong số các điểm từ 10 đến 12, trong đó phương pháp còn bao gồm bước cập nhật, bởi thiết bị truyền thông (304), tiểu sử bảo mật thứ nhất (502) thành tiểu sử bảo mật thứ hai (504) dựa trên ít nhất thay đổi trong trạng thái hoạt động của thiết bị của thiết bị truyền thông (304) hoặc thay đổi trong môi trường mạng của thiết bị truyền thông (304).

14. Phương pháp (200) theo điểm 13, trong đó thông tin cập nhật bảo mật tương ứng với ít nhất một trong: tiểu sử bảo mật thứ hai (504) hoặc một hoặc nhiều khác biệt giữa tiểu sử bảo mật thứ hai (504) và tiểu sử bảo mật thứ nhất (502), và trong đó tiểu sử bảo mật thứ hai (504) bao gồm một hoặc nhiều: các thuộc tính thiết bị cập nhật, trạng thái hoạt động của thiết bị hiện tại, trạng thái hoạt động của thiết bị cuối cùng, đường kết nối mạng thay thế được sử dụng bởi thiết bị truyền thông (304), yêu cầu truy nhập một hoặc nhiều dịch vụ khác với các dịch vụ được hỗ trợ bởi bộ phận bảo mật thứ nhất (420, 610), hoặc sự kiện bảo mật định nghĩa thông tin thay đổi động được liên kết với thiết bị truyền thông (304), và trong đó bộ chỉ báo loại tin nhắn và tiểu sử bảo mật thứ

hai (504) được sử dụng bởi thiết bị mạng (302) để xác định bộ phận bảo mật thứ hai (422, 612) đối với thiết bị truyền thông (304).

15. Phương pháp (200) theo điểm bất kỳ trong số các điểm từ 10 đến 14, trong đó hoạt động gia nhập bộ phận bảo mật thứ hai (422, 612) bao gồm bước thu được, bởi thiết bị truyền thông (304), từ thiết bị mạng (302), một hoặc nhiều trong số: danh sách dịch vụ bảo mật được hỗ trợ bởi thiết bị mạng (302) cho bộ phận bảo mật thứ hai (422, 612), tiểu sử bảo mật bộ phận thứ hai (508) được liên kết với bộ phận bảo mật thứ hai (422, 612), hoặc các tiểu sử bảo mật bộ phận của các bộ phận bảo mật khả dụng với thiết bị mạng (302).

16. Phương pháp (200) theo điểm 15, trong đó hoạt động gia nhập bộ phận bảo mật thứ hai (422, 612) còn bao gồm các bước:

kiểm chứng, bởi thiết bị truyền thông (304), quyết định liên quan đến hoạt động gia nhập bộ phận bảo mật thứ hai (422, 612) dựa trên đánh giá của tiểu sử bảo mật bộ phận thứ hai thu được (508) được liên kết với bộ phận bảo mật thứ hai (422, 612); và

điều khiển, bởi thiết bị truyền thông (304), kích hoạt và vô hiệu hóa một hoặc nhiều chức năng hoặc dịch vụ ở thiết bị truyền thông (304) theo tiểu sử bảo mật bộ phận thứ hai thu được (508) được liên kết với bộ phận bảo mật thứ hai (422, 612), nếu kiểm chứng thành công.

17. Phương pháp (200) theo điểm 10, trong đó thiết bị truyền thông (304) được phân định cho bộ phận bảo mật thứ nhất (420, 610) dựa trên hoạt động gia nhập lần đầu tiên giữa thiết bị truyền thông (304) và thiết bị mạng (302), và trong đó hoạt động gia nhập lần đầu tiên bao gồm bước:

cung cấp, bởi thiết bị truyền thông (304), tiểu sử bảo mật thứ nhất (502) cho thiết bị mạng (302) theo bộ phận thương lượng (418) khi thiết bị truyền thông (304) ở trạng thái không được phân định cho bộ phận bảo mật cụ thể, trong đó tiểu sử bảo mật thứ nhất (502) chỉ báo các khả năng của thiết bị và các

yêu cầu bảo mật của thiết bị truyền thông (304) ở trạng thái không được phân định;

thu được, bởi thiết bị truyền thông (304), lệnh từ thiết bị mạng (302) để gia nhập bộ phận bảo mật thứ nhất (420, 610); và

gia nhập, bởi thiết bị truyền thông (304), bộ phận bảo mật thứ nhất (420, 610) dựa trên lệnh thu được.

18. Thiết bị mạng (302) thực hiện thương lượng bảo mật cho cấu hình mạng bao gồm:

mạch điều khiển (312) được tạo cấu hình để:

thu được thông tin cập nhật bảo mật từ thiết bị truyền thông (304) được phân định cho bộ phận bảo mật thứ nhất (420, 610), bộ phận bảo mật thứ nhất (420, 610) được liên kết với tiểu sử bảo mật bộ phận thứ nhất (506), trong đó thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất (502) của thiết bị truyền thông (304);

xác định bộ phận bảo mật thứ hai (422, 612) đối với thiết bị truyền thông (304) dựa trên thông tin cập nhật bảo mật; và

cấp lệnh cho thiết bị truyền thông (304) để gia nhập bộ phận bảo mật thứ hai được xác định (422, 612).

19. Thiết bị truyền thông (304) thực hiện thương lượng bảo mật cho cấu hình mạng, bao gồm:

mạch điều khiển (318) được tạo cấu hình để:

cấp thông tin cập nhật bảo mật cho thiết bị mạng (302) từ thiết bị truyền thông (304) được phân định cho bộ phận bảo mật thứ nhất (420, 610), bộ phận bảo mật thứ nhất (420, 610) được liên kết với tiểu sử bảo mật bộ phận thứ nhất (506), trong đó thông tin cập nhật bảo mật chỉ báo ít nhất một thay đổi trong tiểu sử bảo mật thứ nhất (502) của thiết bị truyền thông (304);

thu được lệnh từ thiết bị mạng (302) để gia nhập bộ phận bảo mật thứ hai (422, 612); và

gia nhập bộ phận bảo mật thứ hai (422, 612) thỏa mãn ít nhất một thay đổi được chỉ báo trong tiểu sử bảo mật thứ nhất (502) của thiết bị truyền thông (304), dựa trên lệnh thu được.

20. Vật ghi máy tính đọc được bất biến có các lệnh máy tính đọc được được lưu trữ trên đó, các lệnh máy tính đọc được sẽ được thực thi bằng thiết bị máy tính bao gồm phần cứng xử lý để thực thi phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 9.

21. Vật ghi máy tính đọc được bất biến có các lệnh máy tính đọc được được lưu trữ trên đó, các lệnh máy tính đọc được sẽ được thực thi bằng thiết bị máy tính bao gồm phần cứng xử lý để thực thi phương pháp theo điểm bất kỳ trong số các điểm từ 10 đến 17.

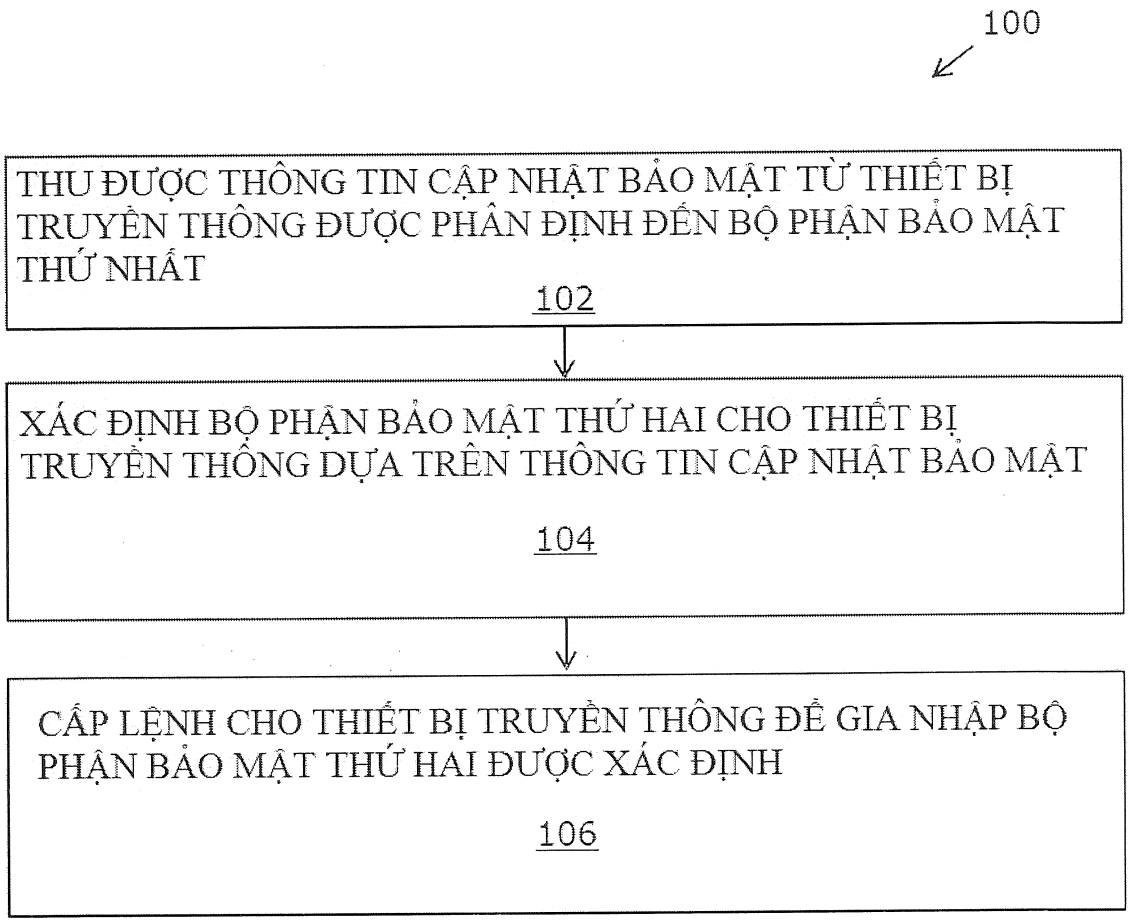
100
THU ĐƯỢC THÔNG TIN CẬP NHẬT BẢO MẬT TỪ THIẾT BỊ TRUYỀN THÔNG ĐƯỢC PHÂN ĐỊNH ĐẾN BỘ PHẬN BẢO MẬT THỨ NHẤT
102
XÁC ĐỊNH BỘ PHẬN BẢO MẬT THỨ HAI CHO THIẾT BỊ TRUYỀN THÔNG DỰA TRÊN THÔNG TIN CẬP NHẬT BẢO MẬT
104
CẤP LỆNH CHO THIẾT BỊ TRUYỀN THÔNG ĐỂ GIA NHẬP BỘ PHẬN BẢO MẬT THỨ HAI ĐƯỢC XÁC ĐỊNH
106

Fig.1

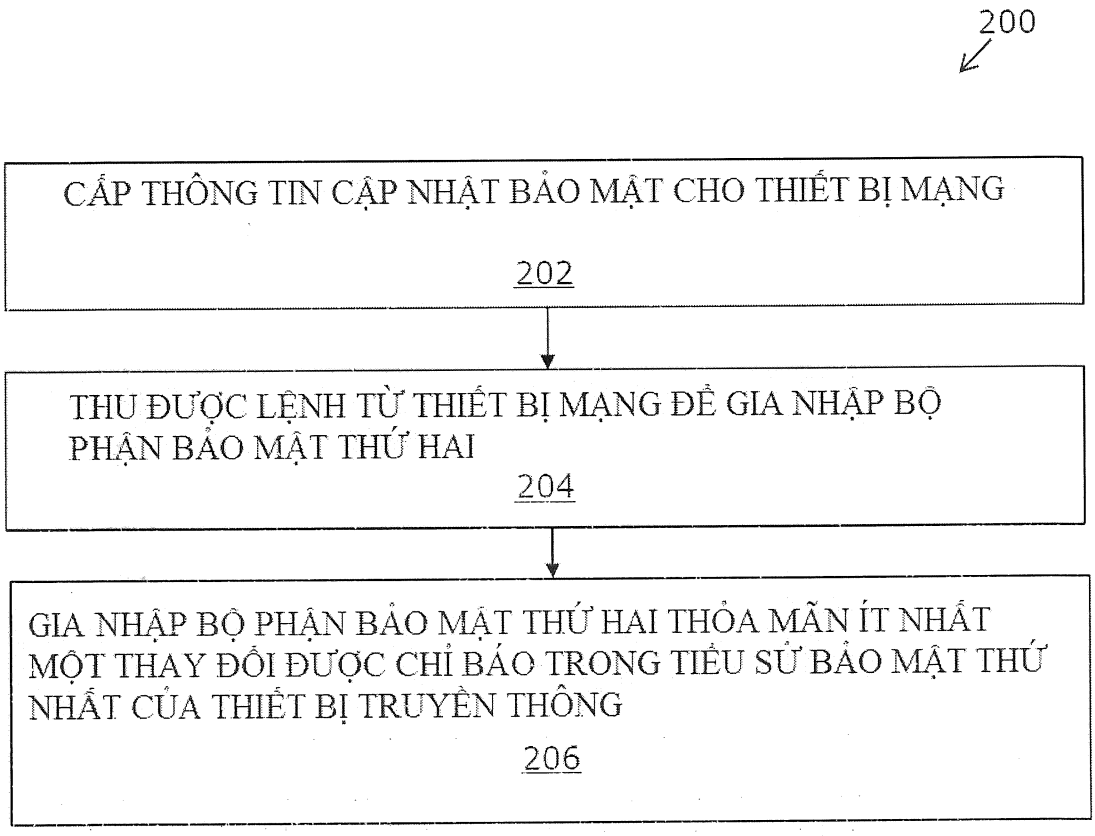
200
CẤP THÔNG TIN CẬP NHẬT BẢO MẬT CHO THIẾT BỊ MẠNG
202
THU ĐƯỢC LỆNH TỪ THIẾT BỊ MẠNG ĐỂ GIA NHẬP BỘ PHẬN BẢO MẬT THỨ HAI
204
GIA NHẬP BỘ PHẬN BẢO MẬT THỨ HAI THỎA MÃN ÍT NHẤT MỘT THAY ĐỔI ĐƯỢC CHỈ BÁO TRONG TIỂU SỬ BẢO MẬT THỨ NHẤT CỦA THIẾT BỊ TRUYỀN THÔNG
206

Fig.2

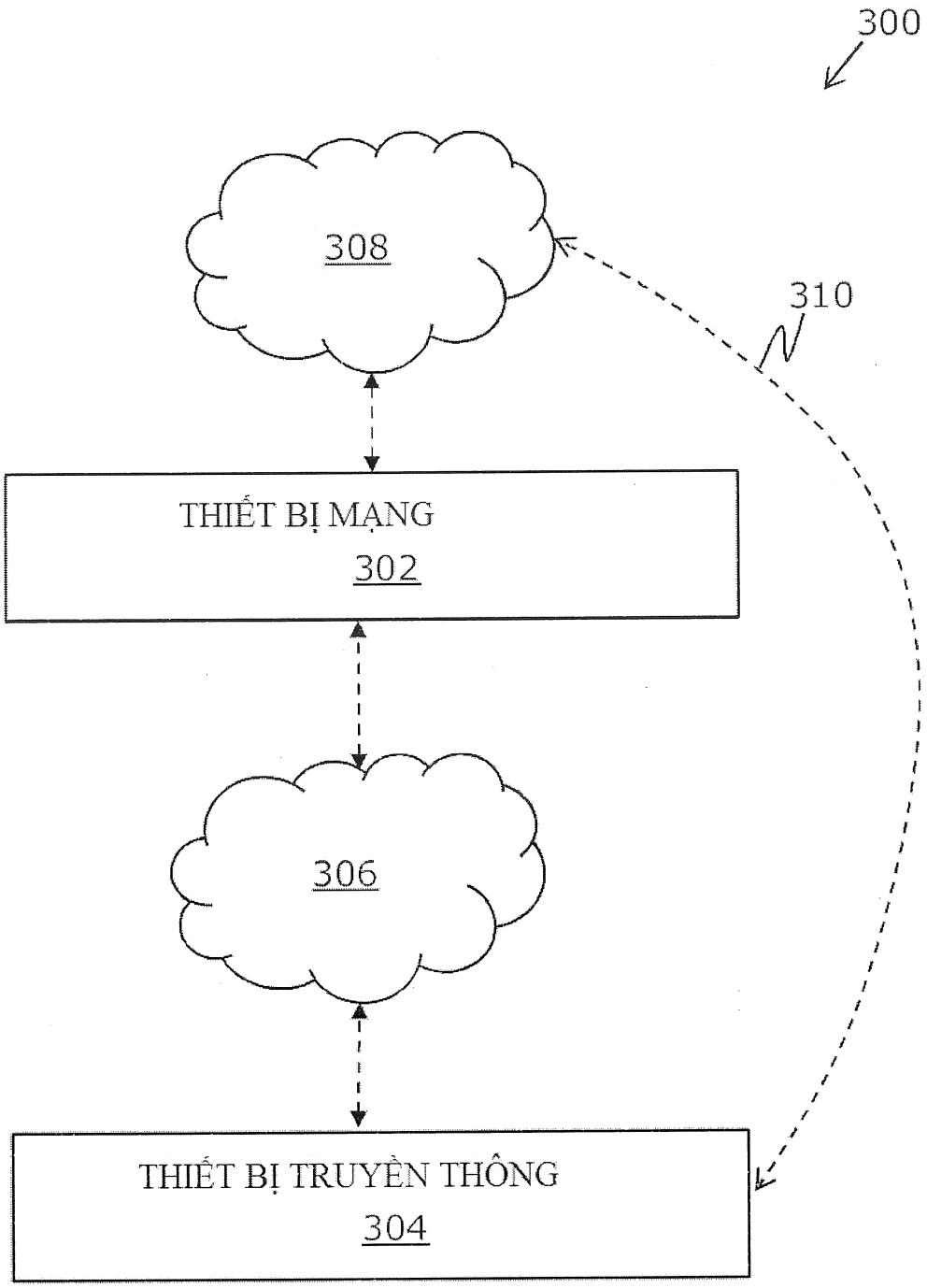

Fig.3A

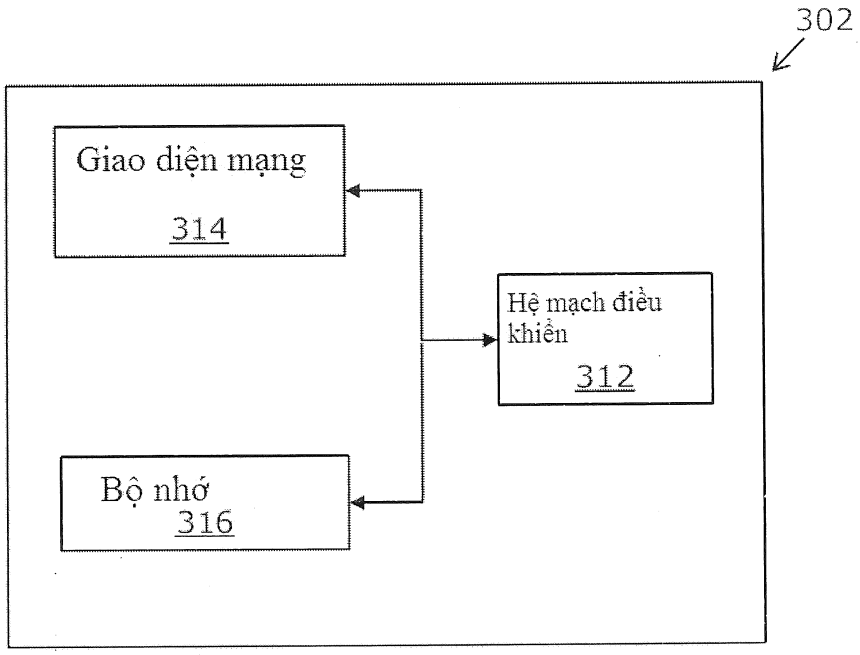
302
Giao diện mạng
314
Hệ mạch điều khiển
312
Bộ nhớ
316

Fig.3B

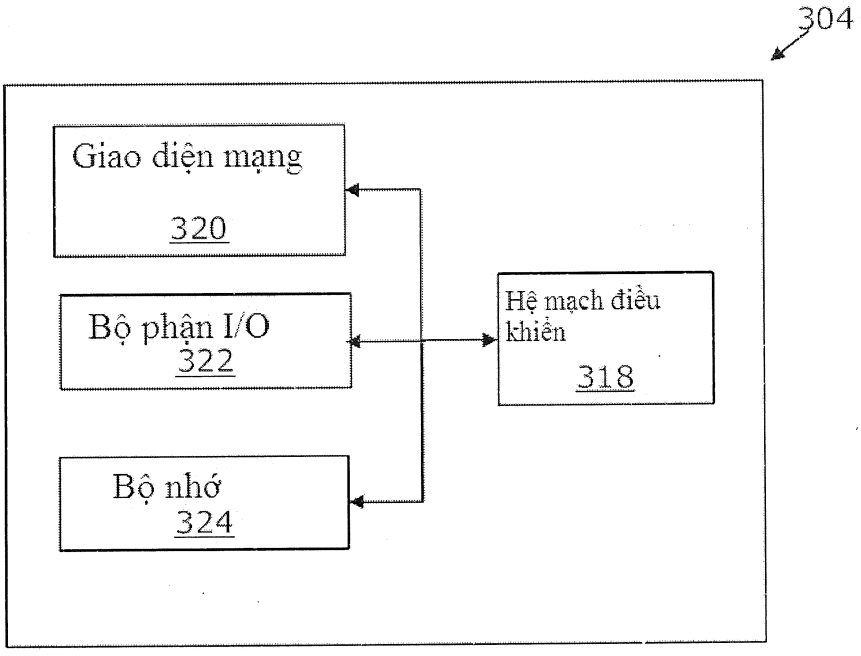
304
Giao diện mạng
320
Bộ phận I/O
322
Hệ mạch điều khiển
318
Bộ nhớ
324

Fig.3C

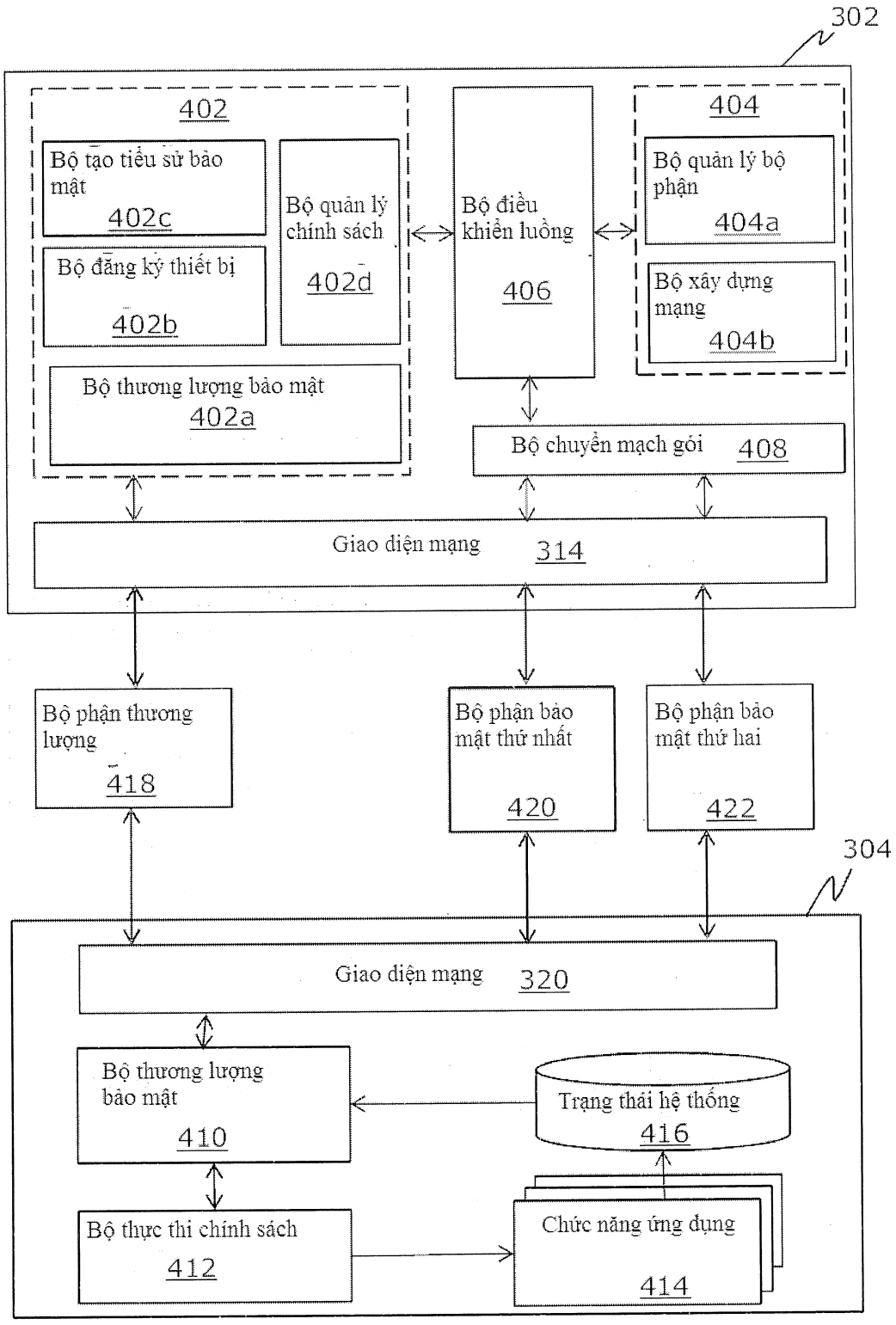
302
402
Bộ tạo tiểu sử bảo mật
402c
Bộ đăng ký thiết bị
402b
Bộ quản lý chính sách
402d
Bộ thương lượng bảo mật
402a
Bộ điều khiển luồng
406
404
Bộ quản lý bộ phận
404a
Bộ xây dựng mạng
404b
Bộ chuyển mạch gói 408
Giao diện mạng 314
Bộ phận thương lượng
418
Bộ phận bảo mật thứ nhất
420
Bộ phận bảo mật thứ hai
422
304
Giao diện mạng 320
Bộ thương lượng bảo mật
410
Trạng thái hệ thống
416
Bộ thực thi chính sách
412
Chức năng ứng dụng
414

Fig.4

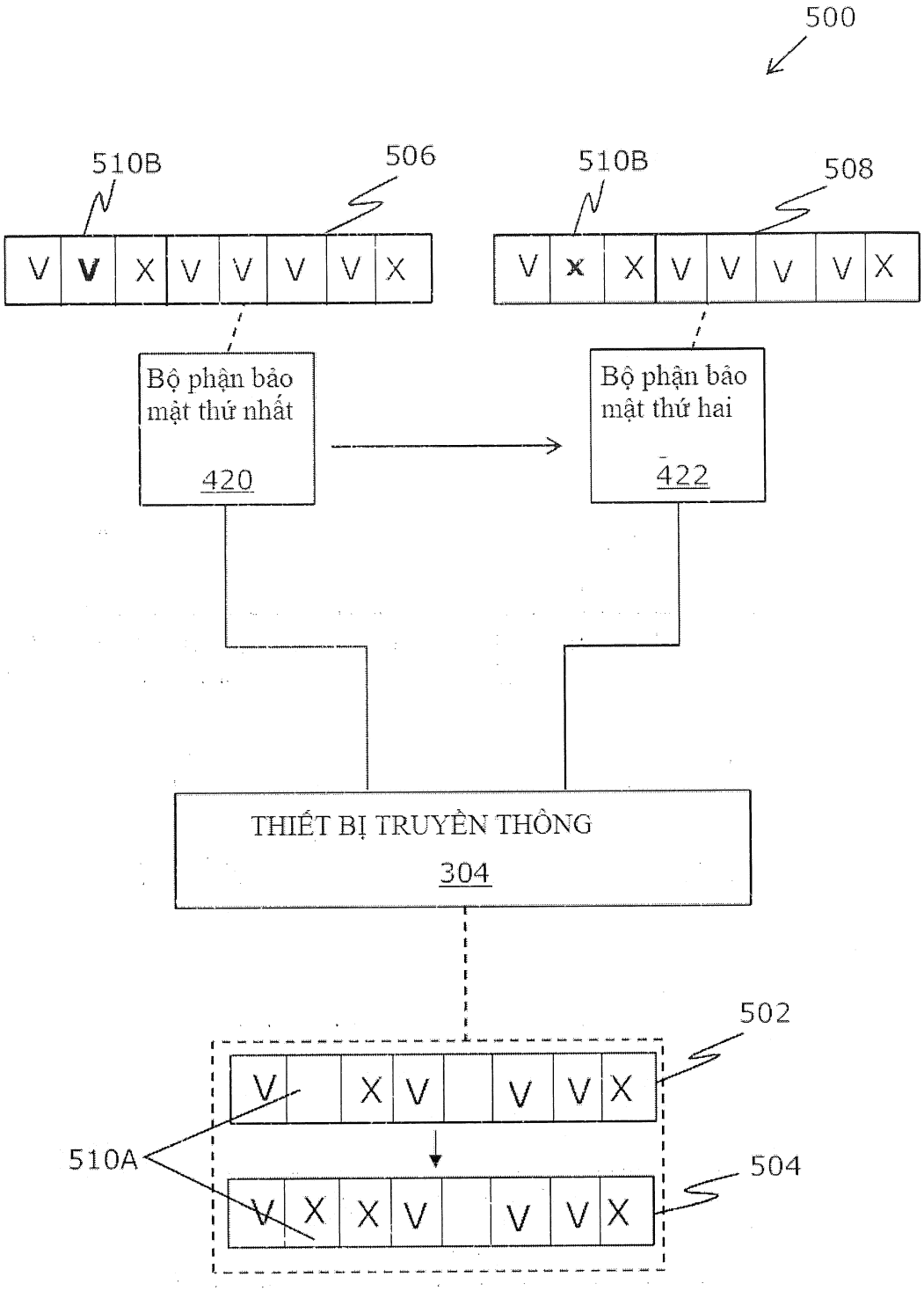
500
510B
506
V V X V V V V X
510B
508
V X X V V V V X
Bộ phận bảo mật thứ nhất
420
Bộ phận bảo mật thứ hai
422
THIẾT BỊ TRUYỀN THÔNG
304
502
V X V V V X
510A
504
V X X V V V X

Fig.5

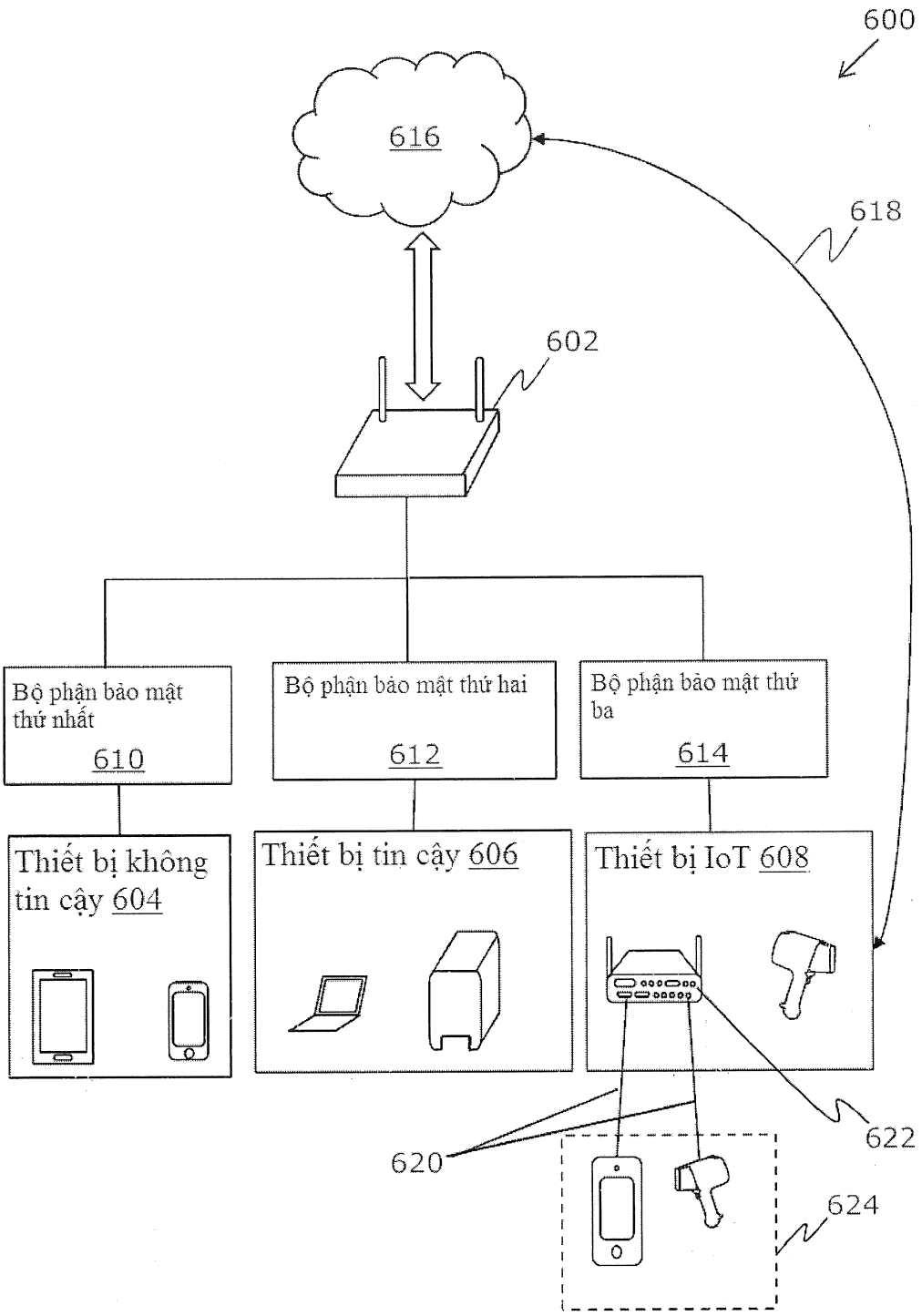
600
616
618
602
Bộ phận bảo mật thứ nhất
610
Bộ phận bảo mật thứ hai
612
Bộ phận bảo mật thứ ba
614
Thiết bị không tin cậy 604
Thiết bị tin cậy 606
Thiết bị IoT 608
620
622
624

Fig.6